UNIVERSIDADE FEDERAL DE SANTA CATARINA

Centro de Ciências da Educação

CURSO DE GRADUAÇÃO EM BIBLIOTECONOMIA

Ismael Cabral

SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS UNIVERSITÁRIAS FEDERAIS:

Um levantamento sobre ferramentas e técnicas utilizadas.

Florianópolis

2015

Ismael Cabral

SEGURANÇA DA INFORMAÇÃO EM BIBLIOTECAS UNIVERSITÁRIAS FEDERAIS:

Um levantamento sobre ferramentas e técnicas utilizadas.

Trabalho de Conclusão do Curso de Graduação em Biblioteconomia, do Centro de Ciências da Educação da Universidade Federal de Santa Catarina, requisito parcial à obtenção do título de Bacharel em Biblioteconomia. Orientação: Prof. Dr. Moisés Lima Dutra.

Florianópolis

2015

Ficha Catalográfica elaborada por Ismael Cabral, graduando no curso de Biblioteconomia da Universidade Federal de Santa Catarina.

C117s Cabral, Ismael
Segurança da Informação em Bibliotecas universitárias federais: um levantamento sobre ferramentas e técnicas utilizadas / Ismael - Florianópolis, 2015.
80 f. : il. ; 30 cm.

Orientador: Prof. Dr. Moisés Lima Dutra.
Trabalho de Conclusão de Curso
(Graduação em Biblioteconomia) – Centro de Ciências da Educação, Universidade Federal de Santa Catarina, Florianópolis, 2015.

Inclui referências

1. Segurança da informação. 2. *Internet*. Globalização. Tecnologia. Bibliotecas Universitárias. Universidades. I. Dutra, Moisés Lima. II. Título.

Acadêmico: Ismael Cabral

Título: Segurança da Informação em bibliotecas universitárias federais: um levantamento sobre ferramentas e técnicas utilizadas.

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Biblioteconomia, do Centro de Ciências da Educação da Universidade Federal de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Biblioteconomia, aprovado com nota 9,5.

Florianópolis, 07 de julho de 2015.

Moisés Lima Dutra, Dr.
Universidade Federal de Santa Catarina
Professor Orientador

Angel Freddy G. Vieira, Dr.
Universidade Federal de Santa Catarina
Titular I da banca examinadora

Enrique Muriel Torrado, Dr.
Universidade Federal de Santa Catarina
Titular II da banca examinadora

Márcio Matias, Dr.
Universidade Federal de Santa Catarina
Suplente da banca examinadora

Este trabalho é dedicado aos meus amados filhos e esposa que foram o meu porto seguro e grandes incentivadores para a realização deste curso de graduação.

AGRADECIMENTOS

Primeiramente a Deus, por seu imensurável amor e justiça e que nos momentos de minhas fraquezas e indecisões me deu força além do natural para prosseguir a caminhada.

Aos meus pais, Amantino Delfino Cabral (*in memoriam*) e Maria Mercedes Cabral que mesmo eu não estando muito presente na vida dela, tenho certeza de que a distância nunca diminuirá o amor e o orgulho que tenho dela.

Aos meus filhos Nícollas, Rhuan e Samuel, que mesmos não compreenderem ainda algumas ausências que tive em alguns momentos na vida deles por razão deste trabalho, sempre estiveram ao meu lado me dando alegrias a amor incondicionais.

A minha amada esposa Sharon Brülinger Pavei Cabral pelo companheirismo, compreensão e paciência que teve comigo ao longo desses quatro anos de curso.

Ao professor Moisés Lima Dutra, por aceitar ser meu orientador neste trabalho.

Aos demais professores do departamento de Ciência da Informação, que foram os alicerces do conhecimento ao longo da minha graduação.

Aos colegas de turma, pela convivência, troca de conhecimentos e pelas amizades que serão sempre lembradas.

E as demais pessoas que, faltar-me-ia espaço para agradecer a força, o incentivo ou até mesmo as críticas recebidas, pois, sem elas um trabalho ou até mesmo a vida, nunca seguirá o caminho da perfeição.

”As pessoas por quem menos esperamos são as que fazem coisas que nunca imaginamos”.

(Alan Turing)

RESUMO

Cabral, Ismael. **Segurança da Informação em Bibliotecas universitárias federais:** um levantamento sobre ferramentas e técnicas utilizadas / Ismael Cabral Florianópolis, 2015. 80 f. : il. ; 30 cm. Orientador: Prof. Dr. Moisés Lima Dutra.
Trabalho de Conclusão de Curso (Graduação em Biblioteconomia) – Centro de Ciências da Educação, Universidade Federal de Santa Catarina, Florianópolis, 2015.

A segurança da informação tem sido uma questão que há muito preocupa o homem, desde a antiguidade aos tempos atuais. Batalhas e guerras foram travadas onde o diferencial para a conquista ou para a derrota foi, na maioria dos casos, o nível de informação ou desinformação que um adversário possuía do outro. Com o advento da internet, a globalização e o rápido desenvolvimento tecnológico das últimas décadas, a informação passou a ser essencial para o homem moderno. A fácil acessibilidade nessa nuvem de informações, em todo lugar e por meio de inúmeros aparelhos eletrônicos, aumentou também significativamente a preocupação em proteger certos dados, informações sigilosas que possam de alguma forma ser acessados por pessoas não autorizadas. Com isso, esta pesquisa analisou e buscou identificar as principais ferramentas e técnicas da segurança da informação mais utilizadas nas bibliotecas universitárias brasileiras. Para tanto, foram enviados questionários via *e-mail* para as instituições, além de pesquisa bibliográfica em meios físicos e eletrônicos. A análise dos resultados demonstrou que apesar de todo o avanço tecnológico dos últimos tempos, a segurança da informação nessas instituições de ensino ainda está muito abaixo do desejado.

Palavras-chave: Segurança da informação. *Internet*. Globalização. Tecnologia. Bibliotecas Universitárias.

ABSTRACT

Cabral, Ismael. **Segurança da Informação em Bibliotecas universitárias federais:** um levantamento sobre ferramentas e técnicas utilizadas / Ismael Cabral Florianópolis, 2015. 80 f. : il. ; 30 cm. Orientador: Prof. Dr. Moisés Lima Dutra.
Trabalho de Conclusão de Curso (Graduação em Biblioteconomia) – Centro de Ciências da Educação, Universidade Federal de Santa Catarina, Florianópolis, 2015.

Information security has been an issue that has long concerned the man, from ancient to modern times. Battles and wars were fought where the differential to conquer or defeat was, in most cases, the level of information or misinformation that an opponent had the other. With the advent of internet, globalization and rapid technological development of recent decades, information has become essential for the modern man. The easy accessibility of information in this cloud, everywhere and through numerous electronic devices, also significantly increased the concern to protect certain data, sensitive information that can somehow be accessed by unauthorized persons. Thus, this research analyzed and sought to identify the main tools and techniques of security the most used information in Brazilian university libraries. To this end, questionnaires were sent via email to the institutions, as well as literature in physical and electronic media. The results showed that despite the technological advances of recent times, information security in these educational institutions is still much lower than desired.

Keywords: Information security. Internet. Globalization. Technology. University Libraries

LISTA DE FIGURAS

Figura 1: Enigma versão da marinha alemã exposta em Bletchley Park.....20
Figura 2: Alan Mathison Turing.....21
Figura 3: Versão reconstruída de uma bombe, ...22
Figura 4: Princípios básicos da segurança da informação.....24
Figura 5: Fatores de sucesso da política de segurança.....28
Figura 6: Happy Hour Virus simula tela azul da morte no Windows.....33
Figura 7: Alerta de Worm em e-mail.....33
Figura 8: Esquema de atuação de bots.....34
Figura 9: Adwares em tela de computador.....35
Figura 10: Cavalo de Troia baixado pela internet.....36
Figura 11: Hoax em uma página do Facebook.....36
Figura 12: Propaganda enviada por Spam em página na Web.....37
Figura 13: Scam instigando a curiosidade de internautas.....37
Figura 14: Phishing em um site de banco.....38
Figura15: Ransomware bloqueando um computador.....39
Figura 16: Rogue simulando proteção em computador.....39
Figura 17: Spyware em computador infectado.....40
Figura18: Falha de segurança que permite a entrada de um backdoor em computador.....41
Figura 19: TrueCrypt, tela do programa para criptografar arquivos.....47
Figura 20: Exemplo de uma assinatura digital.....47
Figura 21: Certificado Digital instalado corretamente.....48
Figura 22: Avira antivírus, protegendo um computador.....50
Figura 23: Filtro Anti-spam bloqueando mensagens potencialmente prejudiciais....50.
Figura 24: Estrutura de atuação de um Firewall.....52

LISTA DE TABELAS

Tabela 1: Resumo comparativo entre os códigos maliciosos.....42
Tabela 2: Incidentes reportados ao CERT.br janeiro a dezembro de 2014.....43

LISTA DE GRÁFICOS

Gráfico 1: Incidentes reportados ao CERT.br – 1999- 2014.....43
Gráfico 2: Meios de controle de acesso às áreas físicas.....55
Gráfico 3: Softwares utilizados no acesso lógico á rede.....56
Gráfico 4: Ferramentas utilizadas ao acesso à rede.....57
Gráfico 5: Circuito fechado de tv monitorando áreas de acesso ao usuário.....58
Gráfico 6: Grau de proteção em segurança da informação na biblioteca.....58
Gráfico 7: Tempo de atualização dos softwares.....59
Gráfico 8: Principais incidentes de segurança reportados.....60
Gráfico 9: Existência de uma política institucional de segurança.....61
Gráfico 10: Existência de uma política de informação.....61
Gráfico 11: Programação de cópias de arquivos.....63
Gráfico 12: Dificuldades em se rastrear ameaças.....64
Gráfico 13: Práticas mais comuns de infecção virtual.....64

SUMÁRIO

1 INTRODUÇÃO **13**
1.1 Justificativa 14
1.2. Objetivos 15
1.2.1 Objetivo Geral 15
1.2.2 Objetivos específicos 15
2 FUNDAMENTAÇÃO TEÓRICA **16**
2.1 Segurança da informação 16
2.1.1 Breve histórico da segurança da informação: da pré-história a Alan Turing 19
2.1.2 Segurança da informação: Princípios 23
2.3 Política de segurança da informação 26
2.3.1 Política de senhas 28
2.3.2 Política de backup 30
2.4 Tipos de ameaças à segurança de informação 32
2.5 Técnicas de segurança de informação 45
2.6 Ferramentas de segurança de informação 49
3 METODOLOGIA **53**
4 RESULTADOS E ANÁLISE DA PESQUISA **55**
5 CONCLUSÕES **67**
REFERÊNCIAS **69**
APÊNDICE A - Questionário **73**
APÊNDICE B - Endereços eletrônicos das bibliotecas **77**

1 INTRODUÇÃO

A chamada era da tecnologia trouxe-nos desenvolvimento em muitas áreas, mas principalmente na da tecnologia de informação e comunicação (TIC). Bianchetti (2008) diz que a informação deixou de ser um meio para alcançar outros fins, tornando-se um fim que se explica e se justifica em si mesmo.

A partir do surgimento da Internet, no período da guerra fria, o mundo vem passando por processos cada vez mais automatizados no que tange ao desenvolvimento tecnológico; isto se deve ao fato de o conhecimento e a comunicação estarem ao alcance de todos quase que instantaneamente, bastando uns cliques no teclado de um computador ligado à rede mundial de computadores. O que surgiu apenas para ser uma forma de comunicação entre as forças armadas americanas, logo adentrou também em suas universidades, com o intuito de fomentar pesquisas e comunicação entre alunos e professores. Entretanto, na década de 1990 a Internet ultrapassou as fronteiras militares e universitárias dos Estados Unidos e ganhou o mundo.

O rápido desenvolvimento científico e tecnológico após a globalização da Internet transformou a maneira como as pessoas e instituições passaram a agir mediante situações que envolvem expor seus dados pessoais e financeiros, mas, sobretudo, os dados que merecem algum sigilo. Isto fez surgir alguns questionamentos em torno da segurança de informação e em como agir mediante difusão de dados pessoais em redes sociais, telefones celulares, cartões de créditos, comércio eletrônico ou em compras em lojas virtuais.

A busca por esta proteção é o meio pelo qual pessoas e instituições se asseguram para poderem trabalhar ou simplesmente navegarem na Internet sem o medo de terem seus dados captados por agentes externos. Este receio não é sem sentido, embora muitas medidas sejam tomadas para tornar um ambiente mais seguro, a questão de segurança de informação será sempre mais complexa do que parece. Assim, de acordo com Oliveira (2001), existem diferenças fundamentais na segurança tecnológica voltada para grandes corporações e para as voltadas aos usuários domésticos. Mas em ambos os casos, a maior preocupação é a de uma invasão em seus sistemas de segurança, ou seja, um ataque externo.

Este cuidado não é diferente em unidades de informação, como por exemplo, em bibliotecas universitárias onde os dados de vários usuários estão registrados e

necessitam de uma proteção contra possíveis invasões ao sistema, assim como aos próprios dados da instituição. Por estes motivos, de acordo com Oliveira (2001), foram criadas as estratégias de segurança, que são passos desenvolvidos para amenizar os riscos ou até mesmo evitar invasões.

Além dessas estratégias de segurança que serão abordadas na pesquisa, também foram desenvolvidas técnicas e ferramentas que auxiliam na proteção de sistemas de segurança de informação. Nakamura (2007, p. 26) lembra que “novas tecnologias e novos sistemas sempre são criados, é razoável considerar que novas vulnerabilidades sempre existirão e, portanto, novos ataques também sempre serão criados”. A segurança de informação ainda é considerada por algumas instituições como um elemento caro e dispensável que não traz um retorno imediato.

1.1 Justificativa

O constante desenvolvimento tecnológico, que traz benefícios, também traz consigo um problema que preocupa tanto pessoas quanto instituições de um modo geral: a segurança da informação. Este termo tem sido muito usado por especialistas da área de tecnologia de informação nas últimas décadas, mas pouco se tem feito para assegurar uma real proteção. Invasões e ataques cibernéticos ocorrem a todo o momento em escala mundial, deixando muitas vezes a vida particular de suas vítimas expostas ao público.

No entanto, após os últimos escândalos de espionagem virtual envolvendo membros do alto escalão político de muitos países e o aumento da preocupação com a privacidade, decorrente deles, a segurança da informação tem se mostrado uma área de grande interesse e também de muitos investimentos e desenvolvimento de tecnologias (NOVAES, 2015). As bibliotecas universitárias, principalmente as que possuem um grande fluxo de acesso à Internet, muitas vezes também são alvos de ataques virtuais. Esta pesquisa levantará informações sobre como está a preocupação das bibliotecas universitárias com a segurança da informação, o que se tem feito a esse respeito, que medidas de segurança são tomadas e quais benefícios essas medidas trazem para a comunidade acadêmica em geral.

Esta pesquisa se justifica, portanto, pelo fato de se procurar saber quais as ferramentas e técnicas de segurança da informação são mais utilizadas nas

bibliotecas universitárias federais do Brasil para garantir o sigilo, tanto dos dados dos usuários nelas registrados, quanto aos das próprias instituições.

1.2 Objetivos

A seguir serão apresentados os objetivos aos quais este trabalho se propôs.

1.2.1 Objetivo geral

O trabalho aqui apresentado tem por objetivo geral identificar as principais técnicas e ferramentas da Segurança da Informação e o grau de utilização destas pelas bibliotecas universitárias federais brasileiras.

1.2.2 Objetivos específicos

a) Determinar as técnicas mais recentes de Segurança da Informação;
b) Identificar as ferramentas mais recentes da Segurança da Informação;
c) Verificar quais são as ferramentas e técnicas da Segurança da Informação utilizadas pelas bibliotecas universitárias federais brasileiras.

2 FUNDAMENTAÇÃO TEÓRICA

O desenvolvimento deste capítulo apresenta a fundamentação teórica utilizada, os assuntos aqui descritos estão de acordo com os objetivos relacionados à pesquisa.

2.1 Segurança da Informação

"Segurança da informação define-se como o de processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados" (OLIVEIRA, 2001, p. 09).

A segurança da informação visa garantir que as informações estejam protegidas contra o acesso por pessoas não autorizadas, estejam sempre disponíveis, e que sejam confiáveis. Há um senso comum de que segurança da informação significa somente fazer segurança contra hackers, vírus, roubo de informações, e invasão de privacidade. Contratam-se técnicos em segurança da informação para fazer o diagnóstico e implementar dispositivos e procedimentos para a segurança do ambiente, sendo que mesmo com esse processo acaba-se por não tratar dos demais riscos que ameaçam as informações. Pode-se dizer que segurança não é uma questão apenas técnica, mas também gerencial e humana.

Para Oliveira (2001), segurança de informações é um item complexo e pode abranger várias situações como erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, etc.

A segurança da informação implica em garantir que as informações (em qualquer formato: mídias eletrônicas, papel e até mesmo em conversações pessoais ou por telefone) estejam protegidas contra o acesso por pessoas não autorizadas (confidencialidade), estejam sempre disponíveis quando necessárias, e que sejam confiáveis (não tenham sido corrompidas ou adulteradas por atos de pessoas mal-intencionadas).

Para que haja segurança das informações, primeiramente deve ser feita uma análise que identifique todos os riscos (vulnerabilidades e ameaças) que pairem sobre as informações. Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: físicos, lógicos e humanos.

Aspectos físicos: Para Adachi (2004), "a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs".

Aspectos lógicos: A camada lógica é caracterizada pelo uso de softwares - programas de computador - responsáveis pela funcionalidade do hardware, pela realização de transações em base de dados organizacionais, criptografia de senhas e mensagens etc. Para Adachi (2004), é nessa camada que estão as "regras, normas, protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas". A segurança, em nível lógico, refere-se ao acesso que indivíduos têm às aplicações residentes em ambientes informatizados, não importando o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são, em sua maior parte, "invisíveis" aos olhos de pessoas externas aos ambientes de informática; estas só os reconhecem quando têm o seu acesso barrado pelo controle de acesso (CARUSO; STEFFEN, 1999).

Aspectos humanos: A camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de Tecnologia da Informação (TI), seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (ADACHI, 2004). Das três camadas, esta é a mais difícil de avaliar os riscos e gerenciar a segurança, pois, envolve o fator humano, com características psicológicas, socioculturais e emocionais, que variam de forma individual (SCHNEIER, 2001). A gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia - hardware e software - envolve pessoas e processos, porém, algumas empresas negligenciam este fator. A política de segurança e a conscientização dos usuários são algumas das formas de se controlar a segurança desta camada.

A segurança da informação é assunto estratégico e deve ser tratado no nível profissional especializado. Em sua forma mais simples, a segurança se preocupa em garantir que pessoas mal-intencionadas leiam ou modifiquem mensagens enviadas a outros destinatários. Outra preocupação da segurança se volta para as pessoas

que tentam ter acesso a serviços remotos, aos quais elas não estão autorizadas (PÉRICAS, 2003).

A segurança da informação também procura antecipar procedimentos que possam por ventura tentar ir contra a política de segurança da organização, garantindo com isso o sigilo da informação e a integridade dos dados.

Grande parte dos problemas de segurança pode ser intencionalmente causada por pessoas que tentam obter algum benefício ou prejudicar alguém. Dentro das empresas um funcionário insatisfeito, por exemplo, poderia eventualmente sabotar um projeto, ou então vender informações para a concorrência, a segurança da informação precisa prever esta situação e adotar medidas para minimizar os riscos envolvidos.

Devemos ter claro que não existe sistema seguro em todos os sentidos. Estamos na era da informação, onde os dados trafegam de maneira bastante intensa nas redes sociais, nos e-mails, sites de pesquisa e outros. Tudo isso em *desktops, notebooks, tablets* e celulares, entre outros. Porém, com tantos meios de comunicação e com o tráfego a todo vapor, surgem algumas questões: Será que estamos seguros? Ou nossas informações particulares estão nas mãos de quem não deveria? E como se resolve isso?

Recentemente, alguns famosos como as atrizes norte-americanas Jennifer Lawrence e Scarlet Johansson tiveram seus celulares ou contas em redes sociais invadidos e as fotos ficaram expostas na *web*. O caso mais famoso no Brasil foi o da exposição de fotos íntimas da atriz Carolina Dieckmann**,** o fato foi tão marcante que a presidente Dilma Rousseff sancionou, em dezembro de 2012, a Lei 12.737/2012, conhecida como ‘Lei Carolina Dieckman’. O texto prevê como crime a invasão à computadores e smartphones em terras brasileiras (NOVAES, 2015).

Oliveira (2001) diz: “o único sistema totalmente seguro é aquele que não possui nenhuma forma de acesso externo, está trancado em uma sala totalmente lacrada da qual uma única pessoa possui a chave. E esta pessoa morreu no ano passado”.

Sabe-se que existem programas de segurança que são pagos, alguns custam muito caro, dependendo da segurança que se deseja e também para qual finalidade será usado, entretanto, existem os programas *OpenSource,* que além de

geralmente serem gratuitos, ainda possuem código aberto para que possam ser melhorados.

O Sistema Operacional mais indicado para quem quer ficar mais seguro em se tratando de computadores, segundo Oliveira (2001), é o LINUX, que possui código aberto e milhões de desenvolvedores no mundo todo trabalham para corrigir as falhas que possivelmente ocorrerão com o sistema e segurança. Porém, apenas o sistema operacional não é o suficiente para proteção, é necessário adicionar várias ferramentas para complementar a segurança.

2.1.1. Breve histórico da segurança da informação: da pré-história a Alan Turing

A preocupação em se deixar uma informação registrada não é atual, de acordo com Oppermann (2009), ela já estava presente nos homens da caverna nos anos 32000 a.C, aproximadamente, onde, as imagens desenhadas nas rochas das cavernas (pictografias) representavam animais, como bisões, cavalos e cervos. Isto indica clara evidência da preocupação em deixar registrados aqueles desenhos de uma forma que o tempo não apagasse.

Ao mesmo tempo, gradualmente, ele foi criando símbolos para retratar situações de seu cotidiano. Esta lenta evolução nas linguagens de comunicação possibilitou o surgimento da escrita.

Com a escrita, surge a necessidade de transmitir mensagens confidenciais, compreendidas apenas pelo emissor e pelo receptor (criptografia). Aparece também o desejo de interceptar mensagens e de decifrá-las. Motivos não faltaram: segredos militares, políticos, religiosos, questões de comércio ou motivos sentimentais (COSTA; FIGUEIREDO, 2010).

Traços de criptografia apareceram, por volta de 2000 a.C, no Egito e na Mesopotâmia. Os sacerdotes egípcios usavam expedientes criptográficos, ao utilizarem a escrita hierática (hieroglífica), incompreensível para o resto do povo que usava língua demótica. Como afirmam Costa e Figueiredo (2010), o mesmo fenômeno é encontrado nos Babilônicos com a escrita cuneiforme.

A preocupação com a informação segura tal como a entendemos nos dias atuais teve seu início em 1918, quando o engenheiro Holandês Arthur Scherbius

patenteou, na Polônia, uma máquina de cifragem usando rotores, que foi chamada de Enigma. A Enigma (Figura 1) foi utilizada na segunda guerra mundial, durante os anos 1930 e 1940. Era um dispositivo rotor eletromecânico de cifras que convertia mensagens puramente texto em um resultado criptografado. A Enigma parecia uma máquina de escrever robusta, mas podia gerar mais de dez trilhões de combinações

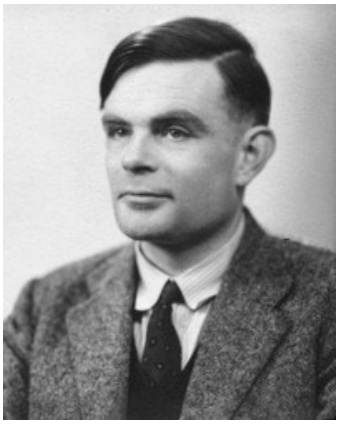
Figura 1 – Enigma versão da marinha alemã exposta em *Bletchley Park*

Fonte: Wikipédia, a enciclopédia livre.

A ideia era construir uma máquina para quebrar códigos de comunicação e realizar vários tipos de cálculos de artilharia para ajudar as tropas aliadas durante a segunda guerra mundial (MORIMOTO, 2011).

Não admira que os alemães considerassem seu código indecifrável. O exército alemão via no dispositivo o potencial de proteger suas comunicações durante o conflito. Os generais de Hitler se comunicavam em absoluto sigilo, até que os códigos utilizados para proteger as mensagens foram descobertos por Alan Turing, cientista da computação britânico (Figura 2).

Figura 2 – Alan Mathison Turing



Fonte: National Portrait Gallery,
Londres, Inglaterra.

Turing que viveu entre as décadas de 1910 e 1950, é considerado um dos pais da Ciência da Computação. No início da Segunda Guerra Mundial, Turing foi recrutado para a Escola de Códigos e Criptogramas do governo inglês. Uma equipe havia sido incumbida de decifrar os códigos militares nazistas, um trabalho urgente e secreto, pois os alemães haviam construído e usavam a máquina "Enigma", que gerava mensagens em códigos indecifráveis. Os código da “Enigma” eram constantemente trocados (GARCIA, 2015).

A complexidade da “Enigma” - que substituía letras com palavras aleatórias escolhidas de acordo com uma série de rotores, estava no fato que seus elementos internos eram configurados em bilhões de combinações diferentes, sendo impossível decodificar o texto sem saber as configurações originais.

Garcia (205), diz ainda que após espiões poloneses roubarem uma cópia da máquina, Turing e o campeão de xadrez Gordon Welchman construíram uma réplica na base militar de *Bletchey Park,* na Inglaterra. A máquina replicava os rotores do sistema alemão e tentava reproduzir diferentes combinações de posições dos rotores para testar possíveis soluções.

Em quatro anos de trabalho, Turing conseguiu quebrar a Enigma ao perceber que as mensagens criptografadas alemãs continham palavras previsíveis, como nomes e títulos dos militares. Turing usava esses termos como ponto de partida, procurando outras mensagens onde a mesma letra aparecia no mesmo espaço em seu equivalente criptografado.

O matemático desenvolveu um sistema chamado *"bombe",* (Figura 3), para traduzir os textos secretos dos alemães, gerados por máquinas de criptografia chamadas de "Enigma". A *bombe* (figura 3), traduzia comunicações codificadas pela Enigma, transformando-as em uma mensagem verdadeira e compreensível.

Figura 3 – Versão reconstruída de uma *bombe,* no Museu de Bletchley Parck, Inglaterra.

Fonte: Wikimédia commons

O primeiro-ministro britânico Winston Churchill, posteriormente, afirmaria que Turing realizou a principal contribuição individual para a vitória dos Aliados.

No entanto, segundo Garcia (2005), desvendar a enigma não foi a única descoberta tecnológica de Turing durante a Segunda Guerra. Em 1944, ele desenvolveu um método para criptografar conversas telefônicas, baseado em um trabalho que ele viu nos laboratórios da *Bell* nos Estados Unidos, em 1942. Chamado de *Deliah*, o sistema nunca foi usado pelo governo inglês. Mas Turing levou parte do trabalho de volta para a Bell quando a empresa desenvolveu o SIGSALY, um dos primeiros aparelhos usados para proteger registros de voz, usado para as comunicações mais confidenciais entre os Aliados.

Para Fontoura (2012), os estudos de Turing se tornaram base para a tecnologia atual.

2.1.2 Segurança da Informação: Princípios

A Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização (ROSA, 2010). Segundo a Norma ISO 27001 (ABNT, 2006), que gerencia a segurança da informação no mundo, a “Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

> Nenhuma área da informática é tão vasta e apreciada como a segurança da informação; o ponto principal da segurança leva a um ponto principal, o ser humano, todo o processo de segurança inicia e tem seu término em um ser humano. Não adianta nada gastarmos fortunas em equipamentos e sistemas de segurança se não conhecermos quem utilizará nossos sistemas, e quem pode ter acesso a eles mesmos sem autorização (OLIVEIRA, 2001, p. 3).

A segurança da informação, de acordo com a NBR ISO/IEC 27002 (ABNT, 2005) está calcada em três princípios básicos (Figura 4) a seguir:

- **Confidencialidade:** É a garantia de que a informação seja acessível somente por pessoas autorizadas, ou seja, somente pessoas devidamente autorizadas pela organização devem ter acesso. A informação deve ser protegida independentemente da mídia que a contenha (impressa ou digital). Deve-se cuidar não apenas da proteção da informação como um todo, mas também de partes da informação que podem ser utilizadas para interferir sobre o todo. No caso da rede, isto significa que os dados, enquanto em trânsito, não serão vistos, alterados, ou extraídos da rede por pessoas não autorizadas.

- **Integridade**: A integridade consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de *status*, remoção e criação de informações. Deve-se considerar a proteção da informação nas suas mais variadas formas, como por exemplo, armazenada em discos ou fitas de backup. Integridade significa garantir que se o dado está lá, então não foi corrompido, encontra-se íntegro. Isto significa que aos dados originais nada foi acrescentado, retirado ou modificado. A integridade é

assegurada evitando-se alteração não detectada de mensagens (Ex: tráfego bancário) e o forjamento não detectado de mensagem (aliado à violação de autenticidade).

- **Disponibilidade:** Consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

Figura 4 – Princípios básicos da segurança da informação.

Fonte: http://segurancadainformacao.modulo.com.br/seguranca-da-informacao

No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um novo ataque (ROSA, 2010).

Na área da segurança da informação, quando há uma potencial ameaça nos princípios que regem seus processos, essa ameaça é denominada como um incidente de segurança da informação, ou seja, é a perda de uma de suas três

características principais, que são, de acordo com a NBR ISO/IEC 27002 (ABNT, 2005).

- **Perda de Confidencialidade:** Quando há uma quebra de sigilo de uma determinada informação (ex: a senha de um usuário ou administrador de sistema) permitindo que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado grupo de usuários.
- **Perda de Integridade**: acontece quando uma determinada informação fica exposta a manuseio por uma pessoa não autorizada, que efetua alterações que não foram aprovadas e não estão sob o controle do proprietário (corporativo ou privado) da informação.
- **Perda de Disponibilidade**: acontece quando a informação deixa de estar acessível por quem necessita dela. É o caso da perda de comunicação com um sistema importante para a empresa que aconteceu pela queda de um servidor, apresentou uma falha devido a erro causado por motivo interno ou externo ao equipamento, ou por ação não autorizada de pessoas com ou sem má intenção.

Conforme afirma Rosa (2010), no caso de ameaças à rede de computadores ou a um sistema, estas podem vir de agentes maliciosos, muitas vezes conhecidos como *crackers* (não se deve confundi-los com os *hackers* que não são agentes maliciosos, pois tentam ajudar a encontrar possíveis falhas nos sistemas).

Estas pessoas são motivadas para fazer esta ilegalidade por vários motivos. Os principais são: notoriedade, autoestima, vingança e o dinheiro.

> A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem. (LAUREANO, 2005, p. 15).

No entanto, garantir a segurança da informação não envolve apenas sistemas computacionais, informações eletrônicas e sistemas de armazenamento, envolve também vários outros aspectos e formas de proteção, monitoramento e cuidado com os dados, como abordará o próximo tópico.

2.3 Políticas de Segurança da Informação

Política de segurança da informação é uma declaração ampla e direta dos objetivos e intenções da organização com relação à conexão de rede e ao seu uso (BRASIL, 2000). Na esfera pública, o Decreto lei n.º 3.505, de 13 de junho de 2000 instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Em seu artigo primeiro, decreta:

> I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
> II - proteção de assuntos que mereçam tratamento especial;
> III - capacitação dos segmentos das tecnologias sensíveis;
> IV- uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
> V- criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
> VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
> VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade (BRASIL, 2000).

De acordo com Nakamura e Geus (2007, p. 188), a política de segurança da informação é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações. Conforme observam ou autores, ela trata dos aspectos humanos, culturais e tecnológicos de uma organização, levando em consideração também, os processos e os negócios, além da legislação local. É com base nessa política de segurança que as diversas normas e os vários procedimentos devem ser criados; a política de segurança é baseada na NBR ISO/IEC17799 (ABNT, 2005).

Caruso (1999) cita os elementos essenciais para a definição de uma política de segurança e para a sua implantação:

- **Vigilância:** Todos os membros da organização devem entender a importância da segurança para a mesma, fazendo com que atuem como guardiões da rede, evitando-se assim, abusos sistêmicos e acidentais.
- **Atitude:** Significa a postura e a conduta quanto à segurança. Sem a atitude necessária, a segurança proposta não terá nenhum valor.

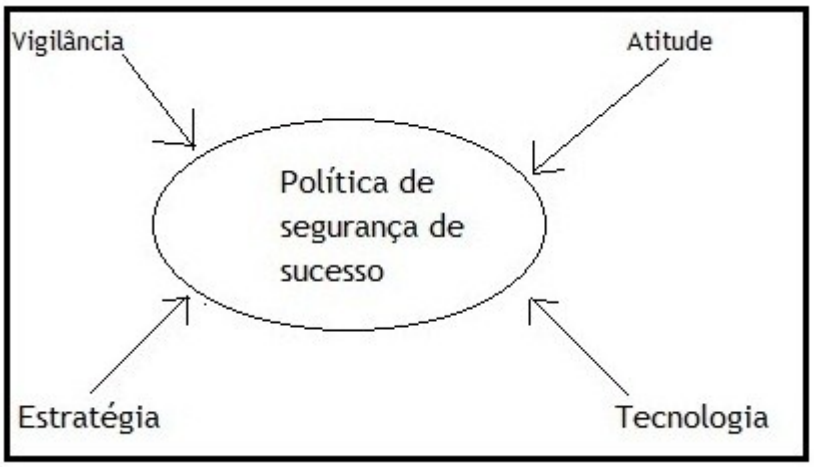
- **Estratégia:** Diz respeito a ser criativo quanto às definições da política e do plano de defesa contra intrusões, além de possuir a habilidade de ser adaptativo a mudanças no ambiente, tão comuns no meio cooperativo.
- **Tecnologia:** A solução tecnológica deve ser adaptativa e flexível a fim de suprir as necessidades estratégicas da organização, pois, qualquer tecnologia um pouco inferior resulta em um falso e perigoso senso de segurança, colocando em risco toda a organização.

De acordo com Fontes (2000), a política de segurança deve ser entendida por todos os funcionários de uma organização. Algumas características fundamentais seriam:

- Informação como um bem da empresa;
- Controle de acesso à informação;
- Definição do gestor da informação;
- Responsabilidades do usuário, da gerência e do gestor da informação;
- Preparação para situações de contingência, garantindo a continuidade da execução de negócio;
- Definição do uso profissional da informação da empresa;
- Definição da possibilidade, ou não, da empresa acessar arquivos pessoais do usuário;
- Definição da identificação do usuário como pessoal e única, bem como a responsabilidade do sigilo da senha;
- Conscientização dos usuários e;
- Medidas disciplinares que serão utilizadas caso a política não seja cumprida.

Assim, como mostra a Figura 5 a seguir, estes elementos podem ser considerados os fatores de sucesso da política de segurança.

Figura 5 – Fatores de sucesso da política de segurança.



Fonte: Nakamura e Geus (2007, p. 193).

Como bem salientam os autores Nakamura e Geus (2007), a política de segurança pode ser considerada o principal elemento para a segurança de informação de qualquer instituição. No próximo capítulo serão conceituadas as políticas de *backup* e de senhas.

2.3.1 Política de senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou *password* é a mais controversa. Elas são utilizadas pela maioria dos sistemas de autenticação e são consideradas necessárias como um meio de proteção. Porém, como afirma Nakamura e Geus (2007, p. 204), elas são consideradas também perigosas, principalmente porque dependem do elo mais fraco da corrente da segurança, os usuários. Assim, num cenário problemático teríamos de um lado profissionais com dificuldade de memorizar várias senhas de acesso, do outro, funcionários displicentes que anotam a senha sob o teclado e a guardam no fundo das gavetas ou, em casos mais graves o colam no próprio monitor.

Recomenda-se, de acordo com a NBR ISO/IEC 27002 (ABNT, 2005), a adoção das seguintes regras para minimizar o problema, sendo que a regra

fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

- Senha com data para expiração: adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.
- Senhas sem repetição: deve-se assegurar através de regras pré-definidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, por exemplo: se a senha anterior for “123senha” a nova senha deverá ter pelo menos 60% dos caracteres diferentes tal como “456seuse”. Neste caso foram repetidos somente os caracteres “s” e “e”, os demais são diferentes.
- Composição com número mínimo de caracteres numéricos e alfabéticos: define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo: “1s4e3u2s” posicional os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos por exemplo: “1432seus”.
- Senhas que não podem ser utilizadas: monta-se uma base de dados com formatos conhecidos de senhas e proíbe-se o seu uso, como por exemplo, se o usuário se chama José da Silva, logo sua senha não deve conter partes do nome como “1221jose” ou “1212silv”.
- Senhas sem formatos pré-definidos: Deve-se evitar a utilização de senhas que combinem com os formatos de datas do calendário, placas, números de telefone, ou outros números comuns, como por exemplo, “DDMMAAAA”, “19XX”, “1883emc”, “I2B3M4”, entre outros.
- Senhas que diferenciem maiúsculas de minúsculas: recomenda-se utilizar senhas *Case Sensitive* (quando os caracteres em caixa alta e baixa são tratados de modos diferentes), e utilização de caracteres especiais como “@ # $ % & *”.
- O uso do nome de uma empresa ou de uma abreviatura, por exemplo: “microsoft123”, “rbstv”.

Ferreira (2008, p.100), diz que “uma boa senha deve ter pelo menos oito caracteres (letras, números e símbolos), deve ser simples de digitar e, o mais importante, deve ser fácil de lembrar”.

2.3.2 Política de backup

Backup é um termo Inglês que tem o significado de cópia de segurança**.** É frequentemente utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos. O *backup* deve ser entendido como um processo especial de salvaguarda do sistema de Tecnologia da Informação e Comunicação.

Assim, o *backup* deve prevenir, então, os equipamentos – *Hardwares* e*,* cópia de arquivos e banco de dados – *Softwares.*

O armazenamento das mídias de *backup*, de acordo com Ferreira e Araújo (2008), deve ser realizado em localidade diferente de onde estão armazenados os equipamentos geradores da informação para não comprometer a integridade dos *backups*. O *backup* pode ajudar contra a perda de equipamentos por danos, furto ou roubo, evitar ações danosas de funcionários e evitar ações de interceptações hackers.

Ferreira e Araújo (2008) afirmam que é necessário, além dos recursos de hardwares e softwares, possuir procedimentos de *backup* das informações. Segundo os autores, os procedimentos de backup podem ser divididos em três tipos: *completo, incremental e diferencial.*

- ***Backup* completo:** Também chamado de Integral ou Normal. Este tipo de procedimento de cópia de segurança consiste em copiar todos os arquivos para uma mídia apropriada, previamente destinada. Se os dados e arquivos que estão sendo copiados nunca mudam, cada *backup* completo será igual aos outros, ou seja, os arquivos copiados serão iguais. Esse fato ocorre devido ao fato de que um *backup* completo não verifica se o arquivo foi

alterado desde o último *backup*; copia tudo indiscriminadamente para a mídia de *backup*, tendo modificações ou não nos dados e arquivos. Esta é a razão pela qual os backups completos não são feitos o tempo todo: todos os arquivos são gravados na mídia de backup, ocupando grande espaço e quantidade de mídias, o que inviabiliza o sistema de cópia. Isto significa que uma grande parte da mídia de backup é usada mesmo que nada tenha sido alterado, por este motivo os backups incrementais e diferenciais foram criados.

- ***Backup* incremental:** Ao contrário dos *backups* completos, os procedimentos de cópias do tipo incremental primeiro verificam se o horário de alteração de um arquivo é mais recente que o horário de seu último *backup*. Se não for, isto significa que o arquivo não foi modificado desde o último *backup*, assim pode ser ignorado desta vez, ou seja, não será realizado o procedimento de cópia de segurança. Se a data de modificação é mais recente que a data do último *backup,* isto significa que o arquivo foi modificado e deve ter seu *backup* realizado.

- ***Backup* diferencial:** São similares aos *backups* incrementais, pois ambos fazem cópias de arquivos modificados. No entanto, os procedimentos de cópia do tipo diferencial são acumulativos, em outras palavras, toda vez que um arquivo for modificado, este continuará a ser incluso em todos os *backups* diferenciais. Assim como a estratégia utilizada nos *backups* incrementais, os *backups* diferenciais normalmente seguem a mesma tática: um único *backup* completo periódico seguido de *backups* diferenciais mais frequentes.

Para Dias (2000), a política de *backup* contém os procedimentos e a infraestrutura necessários à proteção de todo o acervo informacional da instituição, com o objetivo de possibilitar a continuidade de suas atividades.

2.4 Tipos de ameaças à segurança de informação

De acordo com Bittencourt (2013), a expressão "*malware*" provém do termo "*malicious software*" (do inglês *software* malicioso), que são programas desenvolvidos para executarem ações danosas e ilícitas em um sistema. Entre os danos mais conhecidos, podem ser destacados a perda de dados e o roubo de informações sigilosas. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador, conforme explica a *cartilha de segurança para a internet* (CERTBR, 2014) são:

- Pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto-execução de mídias removíveis infectadas, como *pen-drives*;
- Pelo acesso às páginas *Web* malicioso, utilizando navegadores vulneráveis;
- Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos, ainda de acordo com a mesma cartilha (CERTBR, 2014), são para a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.

Os principais tipos de *malwares* seguem os seguintes princípios de classificação, conforme ESET-companhia Global de Soluções de Software de Segurança (2012):

Vírus: Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando

parte de outros programas e arquivos e, se tornam então, “hospedeiros” do vírus. A Figura 6 exibe a conhecida “tela mortal” do *Windows.*

Figura 6 – *Happy Hour Virus*
simula tela azul da morte no *Windows*

Fonte: Techtudo.com.br

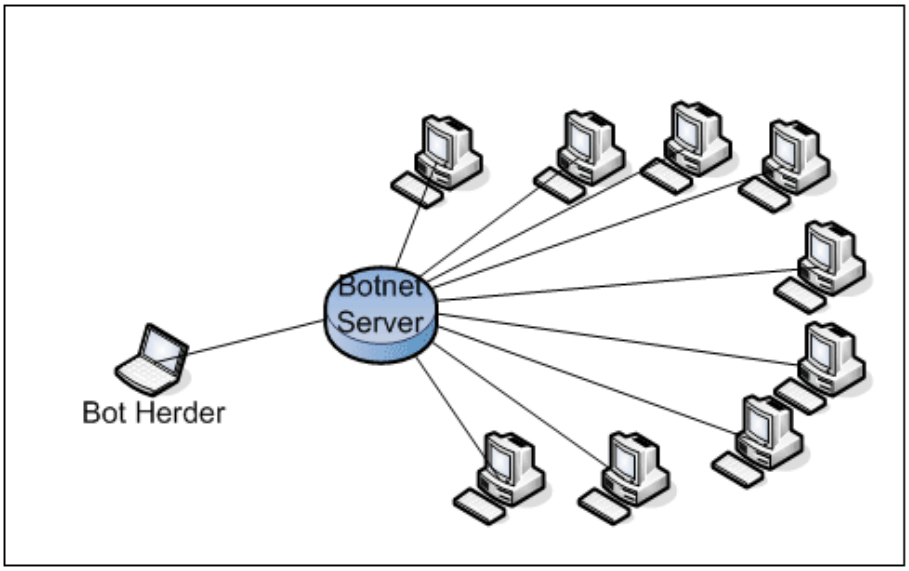
Worms: Na terminologia da informática, os *worms* são na realidade um sub-conjunto de *malware*. Sua diferença principal com os vírus reside no fato de que não necessitam de um arquivo hospedeiro para continuarem vivos. Os *worms* (Figura 7) podem reproduzir-se utilizando diferentes meios de comunicação como as redes locais ou os correios eletrônicos. O arquivo malicioso pode, por exemplo, copiar-se de uma pasta para outra ou enviar-se para toda a lista de contatos de email.

Figura 7 – Alerta de *Worm* em *e-mail*

Fonte: http://security-wire.com/

- **Bot e botnets:** *Bot* (abreviatura do inglês, *robot*, robô), é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores. *Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da *botnet* mais potente ela será. A Figura 8 abaixo, demonstra a arquitetura de atuação de *bots*. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Figura 8 – Esquema de atuação de *bots*



Fonte: http://forum.antinovaordemmundial.com/

- **Adware** (contração de *ADvertisement* - anúncio - e *softWARE*): é um programa malicioso, que se instala nos computadores sem que o usuário perceba e cuja função é baixar ou exibir anúncios publicitários na tela da vítima (Figura 9).

Figura 9 – Adwares em tela de computador

Fonte: blogdoluguta.wordpress.com

- **Cavalo de Tróia:** O nome desta ameaça vem da lenda de um grande cavalo de madeira usado pelos gregos durante a Guerra de Troia, estratégia decisiva para a conquista da cidade fortificada de Tróia. Tomado pelos troianos como um símbolo de sua vitória, foi carregado para dentro das muralhas, sem saberem que em seu interior se ocultava o inimigo. À noite, guerreiros gregos saem do cavalo, dominam as sentinelas e possibilitam a entrada do exército, levando a cidade à ruína (WIKIPÉDIA, 2014). O objetivo deste *software*, então, é o de enganar o usuário. São arquivos que parecem ser normais e inofensivos, e podem ser jogos ou programas que aliciam o usuário a executar determinado arquivo. Desta forma, conseguem instalar-se nos sistemas. Porém, uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo sobre a máquina infectada. A Figura 10 mostra a ameaça de um cavalo de Tróia tentando instalar-se em um computador.

Figura 10 – Cavalo de Troia baixado pela internet

Fonte: *www.linhadefensiva.org*

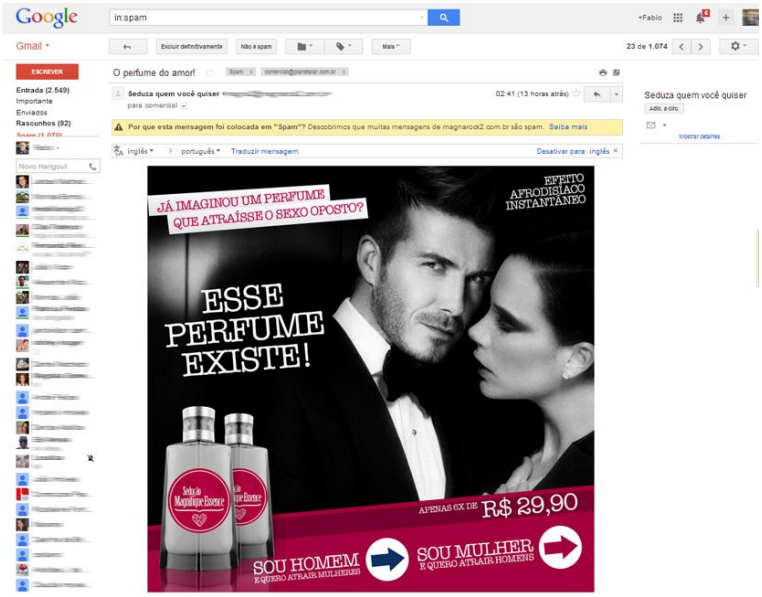
- **Hoax:** um *hoax* (em Português: “mentira”), é um correio eletrônico distribuído em cadeia, cujo objetivo é fazer parecer para os leitores que uma mentira é algo real. Sua diferença para outros tipos de ameaças, como o *phishing, (*ver abaixo), por exemplo, é que os *hoax* (Figura 11) não têm fins lucrativos, pelo menos como finalidade principal.

Figura 11 – *Hoax* em uma página do *Facebook*.

Fonte: www.linhadefensiva.org

- **Spam:** Denomina-se *spam* o correio eletrônico não solicitado enviado massivamente por parte de um terceiro. Em Português, também é identificado como correio indesejado ou lixo. A Figura 12 mostra o aparecimento de um comercial não desejado em uma página na *Web*.

Figura 12 – Propaganda enviada por *Spam* em página na *Web*.



Fonte: http://www.planetalar.com.br/

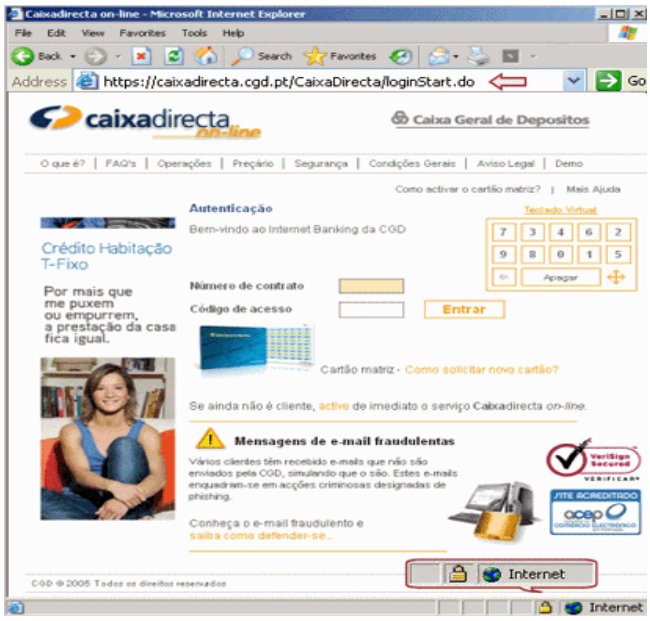
Scam: É a mensagem enviada em massa, à moda do *spam*, com um diferencial: ela contém arquivo anexado ou *link* de condução para um *download* de arquivo. Esse arquivo proporciona a instalação de um cavalo de Troia na máquina do usuário. As mensagens que escondem o *scam* (Figura 13), têm características próprias de instituições financeiras, sítios de cartões de mensagens, notificações de órgãos públicos, notícias de destaque, *downloads* de programas, promoções e eventos, temas pornográficos e mensagens pessoais, sempre com o intuito de deixar as vítimas curiosas ou instigadas.

Figura 13 – *Scam* instigando a curiosidade de internautas

Fonte: *http://www.planetalar.com.br/*

Phishing: Consiste no roubo de informação pessoal e/ou financeira do usuário, através da falsificação de um órgão de confiança (Figura 14). Desta forma, o usuário acha que está entrando os dados em um site de confiança quando, na verdade, estes são enviados diretamente ao atacante.

Figura 14 – *Phishing* em um site de banco



Fonte: http://www.crimelandia.com/

- **Ransomware:** É uma das ameaças cibernéticas mais similares a um ataque sem meios tecnológicos: o sequestro. Em seu aplicativo, o *ransomware* é um código malicioso que codifica as informações do computador e insere nelas uma série de instruções para que o usuário possa recuperar seus arquivos. A vítima, para obter a senha que libera a informação, deve pagar ao atacante uma soma de dinheiro, seguindo as informações que ele disponibiliza. A Figura 15 exibe o *Ransomware* simulando uma página oficial do FBI (*Federal Bureau Investigation*), a polícia federal americana.

Figura 15 – *Ransomware* bloqueando um computador

Fonte: http://www.crimelandia.com/

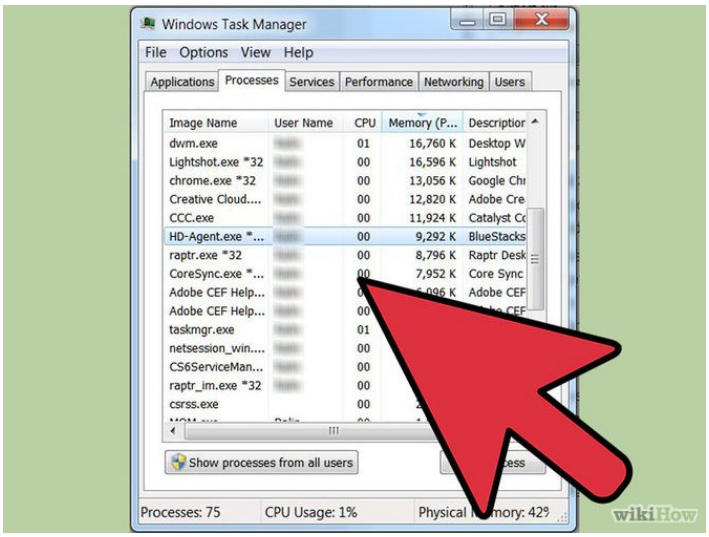
- **Rogue:** É um *software* que, simulando ser um aplicativo *anti-malware* (ou de segurança), tem justo os efeitos contrários: instala um *malware*. Em geral são ataques que exibem na tela do usuário propagandas chamativas sobre a existência de infecções em seu equipamento, como mostra a Figura 16 abaixo. O usuário é convidado a baixar uma solução, às vezes até pagar por ela. Os objetivos da instalação variam desde a instalação adicional de *malwares* até a obtenção de dinheiro através do ataque, dependendo do caso.

Figura 16 – *Rogue* simulando proteção em computador

Fonte: http://malwarerid.com.br/

- **Spyware** (programas espiões): São aplicativos que recopilam informações do usuário, sem seu consentimento. A Figura 17 exibe um *spyware* instalado em um computador. O uso mais comum destes aplicativos é a obtenção de informação do usuário inserido na Internet e o posterior envio da informação arrecadada a entidades externas.

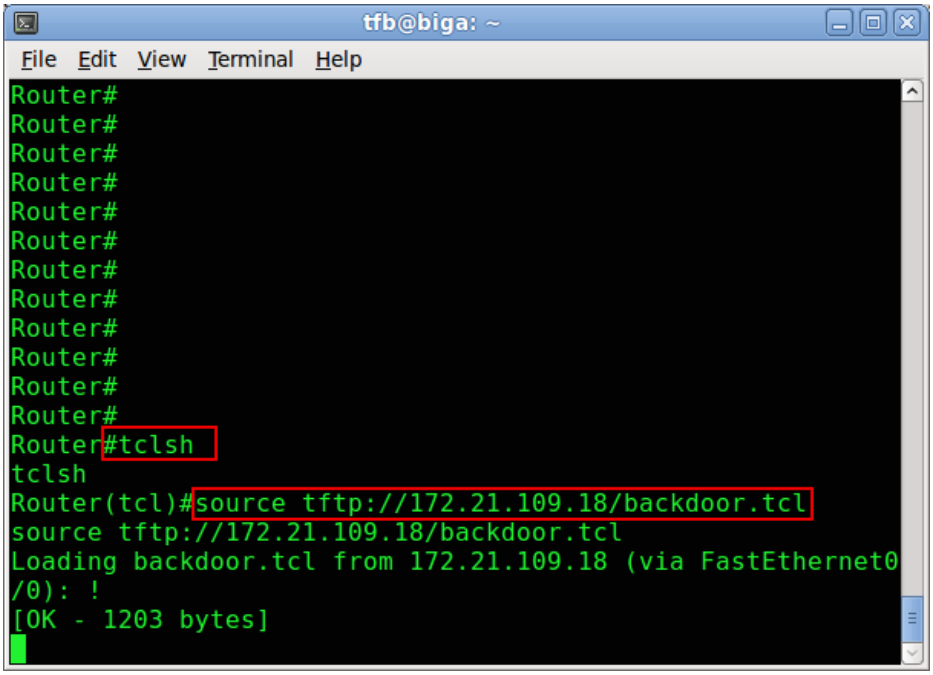
Figura 17 – *Spyware* em computador infectado



Fonte: http://malwarerid.com.br/

- **Backdoor:** Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que exploram vulnerabilidades existentes nos programas instalados no computador para invadi-lo (Figura 18). Após, incluído o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

Figura 18 – falha de segurança que permite a entrada de um *backdoor* em computador



Fonte: http://www.spiasoftware.com/

- **Rootkit:** É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Assim, *rootkit* é uma combinação de todas as técnicas anteriores, pois, o invasor terá acesso privilegiado ao sistema.

A Tabela 1, o Gráfico 1 e a Tabela 2 trazem um comparativo de acordo com o Cert.br (2014), entre os principais códigos maliciosos e sua forma de infecção, os principais incidentes reportados entre os anos de 1999 à 2014 e os incidentes reportados nos meses de janeiro a dezembro de 2014, respectivamente.

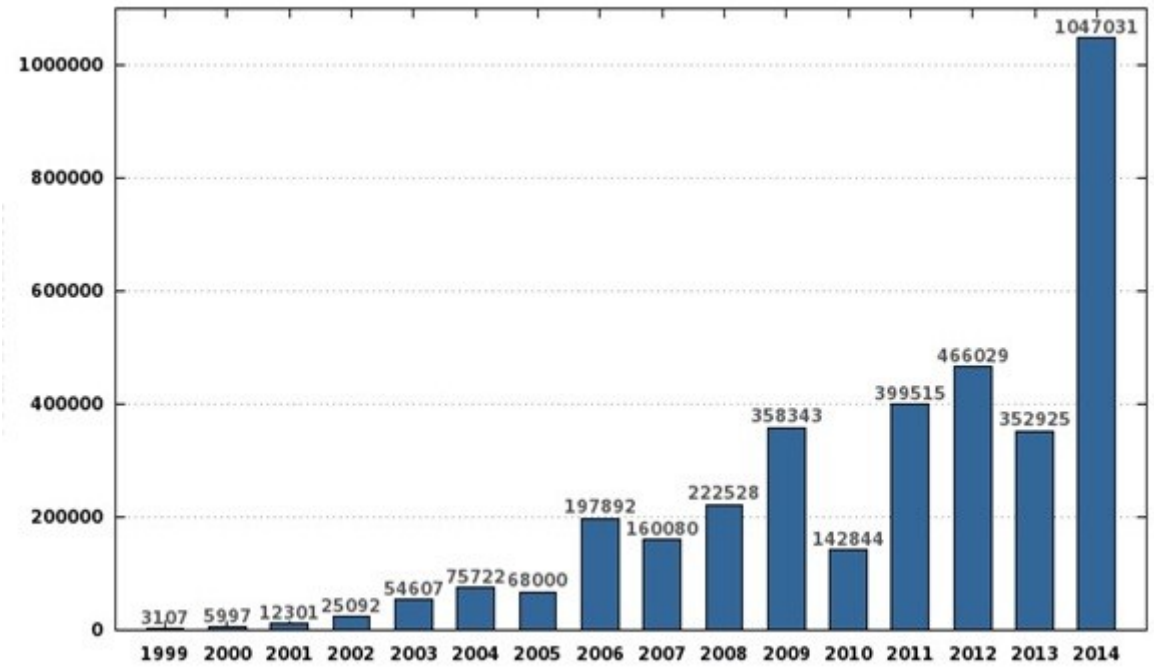
É interessante notar que no Gráfico 1, no ano de 2014, os incidentes reportados tiveram um aumento significativo, levando-se em consideração os anos anteriores.

Tabela 1 - Resumo comparativo entre os códigos maliciosos.

Códigos Maliciosos							
	Vírus	*Worm*	*Bot*	*Trojan*	*Spyware*	*Backdoor*	*Rootkit*
Como é obtido:							
Recebido automaticamente pela rede		✔	✔				
Recebido por *e-mail*	✔	✔	✔	✔	✔		
Baixado de *sites* na Internet	✔	✔	✔	✔	✔		
Compartilhamento de arquivos	✔	✔	✔	✔	✔		
Uso de mídias removíveis infectadas	✔	✔	✔	✔	✔		
Redes sociais	✔	✔	✔	✔	✔		
Mensagens instantâneas	✔	✔	✔	✔	✔		
Inserido por um invasor		✔	✔	✔	✔	✔	✔
Ação de outro código malicioso		✔	✔	✔	✔	✔	✔
Como ocorre a instalação:							
Execução de um arquivo infectado	✔						
Execução explícita do código malicioso		✔	✔	✔	✔		
Via execução de outro código malicioso						✔	✔
Exploração de vulnerabilidades		✔	✔			✔	✔
Como se propaga:							
Insere cópia de si próprio em arquivos	✔						
Envia cópia de si próprio automaticamente pela rede		✔	✔				
Envia cópia de si próprio automaticamente por *e-mail*		✔	✔				
Não se propaga				✔	✔	✔	✔
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✔			✔			✔
Consome grande quantidade de recursos		✔	✔				
Furta informações sensíveis			✔	✔	✔		
Instala outros códigos maliciosos		✔	✔	✔			✔
Possibilita o retorno do invasor						✔	✔
Envia *spam* e *phishing*			✔				
Desfere ataques na Internet		✔	✔				
Procura se manter escondido	✔				✔	✔	✔

Fonte: Cartilha.cert.br

Gráfico 1: Incidentes reportados ao CERT.br – 1999- 2014



Fonte: http://www.cert.br/stats/incidentes/

Tabela 2: Incidentes reportados ao CERT.br janeiro a dezembro de 2014

Mês	Total	worm (%)		dos (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**33959**	2853	8	6539	19	590	1	1267	3	13916	40	7248	21	1546	4
fev	**43227**	4163	9	6190	14	764	1	1434	3	19862	45	9616	22	1198	2
mar	**45808**	9238	20	2829	6	780	1	1253	2	22471	49	7780	16	1457	3
abr	**41533**	3513	8	1505	3	1559	3	1900	4	23320	56	8562	20	1174	2
mai	**48565**	2857	5	8383	17	293	0	1997	4	20756	42	12962	26	1317	2
jun	**54057**	2274	4	10345	19	612	1	2171	4	17477	32	20149	37	1029	1
jul	**58662**	3294	5	10218	17	210	0	2225	3	20292	34	21265	36	1158	1
ago	**134156**	3327	2	38822	28	187	0	1828	1	21500	16	67480	50	1012	0
set	**214954**	3312	1	56184	26	290	0	2347	1	21498	10	130108	60	1215	0
out	**206148**	2563	1	50195	24	296	0	3029	1	23763	11	125060	60	1242	0
nov	**107219**	2571	2	29566	27	201	0	3416	3	28053	26	42420	39	992	0
dez	**58743**	2226	3	3159	5	727	1	5941	10	30751	52	14971	25	968	1
Total	**1047031**	42191	4	223935	21	6509	0	28808	2	263659	25	467621	44	14308	1

Fonte: http://www.cert.br/stats/incidentes/

Legenda da Tabela 2:

- **Worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **Dos** (*Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **Invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **Web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **Scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **Fraude**: segundo o Dicionário Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **Outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que não se deve confundir ***Scan*** com ***Scam***. *Scams* (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

Para Oliveira (2001, p. 151), a segurança da informação deve ser tratada como uma atividade contínua, sempre existirá novas técnicas de ataques da informação e devemos estar prontos para um contra-ataque.

2.5 Técnicas de Segurança da Informação

Automaticamente, ao vermos o termo controle de segurança, logo nos vem à imagem de um guarda restringindo ou liberando o acesso de pessoas à determinado local (SANTOS, 2012). Na segurança da informação não é diferente, existem meios para se controlar o acesso a determinados locais, equipamentos ou softwares. Esses meios podem ser caracterizados por três controles: *administrativo, físico e lógico.*

Controles administrativos: Neste tipo de controle, a administração da instituição deve estabelecer quais regras básicas devem existir, delegando a responsabilidade de criação de controles e o desenvolvimento de procedimentos, padrões e diretrizes. Também devem ser criadas formas de validação dos controles.

Controles físicos: de acordo com Pinheiro (2009), a segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Ela deve se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícita como uma sala, cofre, ou implícita, como áreas de acesso restrito. Ou seja, são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta. (MACÊDO, 2012).

Existem mecanismos de segurança que apoiam os controles físicos: Portas, trancas, paredes, blindagem, guardas, etc.

Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal-intencionado (MACÊDO, 2012).

Para Macêdo (2012), existem mecanismos de segurança que apoiam os controles lógicos:

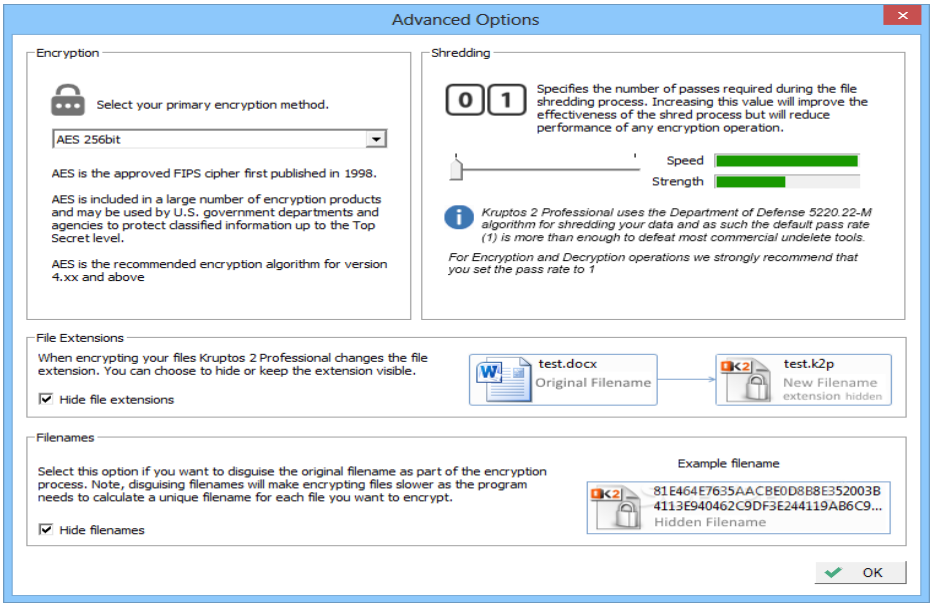
- ***Mecanismos de cifração ou encriptação***: Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. A operação inversa é a decifração.

- ***Mecanismos de garantia da integridade da informação****:* Usando funções de *"Hashing"* ou de checagem, é garantida a integridade através de comparação do resultado do teste local com o divulgado pelo autor.
- ***Mecanismos de controle de acesso***: Palavras-chave, sistemas biométricos*, firewalls*, cartões inteligentes.
- ***Mecanismos de certificação***: Atesta a validade de um documento.
- ***Integridade***: Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.

Algumas das técnicas de segurança da informação que ajudam no controle lógico são:

Criptografia: É definida por (UCHOA, 2005) como a arte e ciência de manter mensagens seguras. De acordo com o mesmo autor, sistemas criptográficos são necessários para evitar uma série de problemas de espionagem nas comunicações eletrônicas. A criptografia consiste basicamente da cifragem dos dados (bits) e/ou codificação destes, tornando-os ilegíveis caso o destinatário não possua a chave secreta responsável por reverter o processo criptográfico. A Figura 19 apresenta a tela do programa *Kruptos 2* que serve para criptografar arquivos.

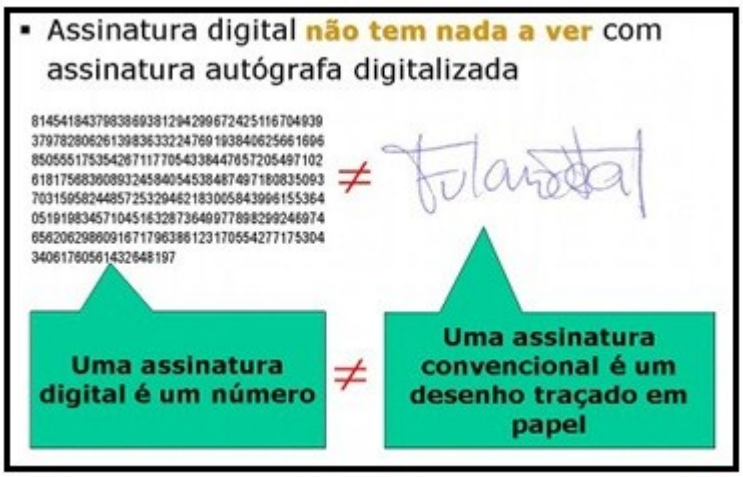
Figura 19 – *Kruptos 2*, tela do programa para criptografar arquivos



Fonte: http://www.softpedia.com/

Assinatura Digital: Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade. Uma assinatura digital não permite o repúdio, isto é, o emitente não pode alegar que não realizou a ação, considerando sua assinatura digital. A Figura 20 mostra a imagem de uma assinatura digital, que é um método de certificação de informação.

Figura 20 – Exemplo de uma assinatura digital

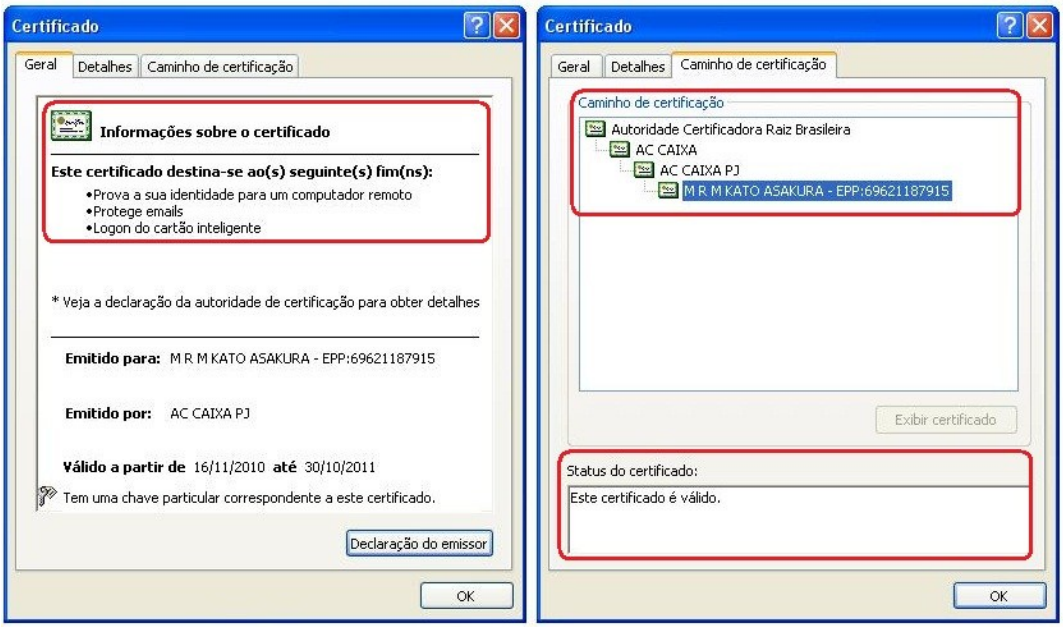


Fonte: http://blog.tempest.com.br/marco-carnut/primeira-metade-assinaturas-digitais.

Certificado Digital: O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Um certificado digital pode ser comparado a um documento de identidade, por exemplo, o passaporte, no qual constam os dados pessoais e a identificação de quem o emitiu. No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal. No caso do certificado digital esta entidade é uma Autoridade Certificadora (AC). A Figura 21 a seguir, mostra a instalação de um certificado eletrônico que serve para a comprovação mútua de identidade.

Figura 21 - Certificado Digital instalado corretamente



Fonte: flexdocs.com.br/guiaNFe/certificado.cliente.html

Esteganografia: É a arte de esconder uma mensagem dentro de uma imagem, vídeo ou qualquer outro tipo de arquivo, fazendo com que esta mensagem passe despercebida aos olhos de terceiros. Esta técnica de segurança da

informação tem como objetivo principal ocultar uma evidência em lugares que não levantariam suspeitas.

Um dos métodos principais para esse processo é usar os bits menos significativos do objeto portador como imagem, vídeo, música entre outros itens que geralmente não levantariam suspeitas aos olhos humanos, para substituir com os bits da informação a ser escondida. Um dos meios mais utilizados é a utilização de programas de esteganografia disponíveis na própria Internet.

No entanto, esta técnica vem sendo utilizada também para propósitos ilegais, tais como, roubo de dados, encapsulamento de vírus, proteção de arquivos pornográficos, pedofilia e entre outros.

Assim, os mecanismos de controles juntamente com as técnicas de segurança são mais um dos métodos que auxiliam na segurança de informação.

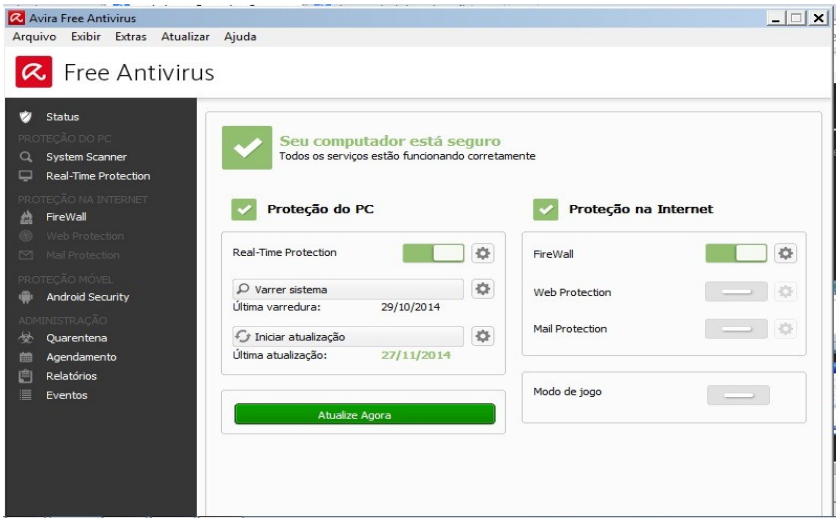
2.6 Ferramentas de Segurança da Informação

As ferramentas de segurança da informação “São um conjunto de softwares, hardwares e técnicas que tem por objetivo combater ataques virtuais” (CHESWICK, 2005, p. 143-334). Podem ser encontradas nas plataformas de sistema operacional como Microsoft Windows e Linux. Dentre as inúmeras ferramentas encontradas, destacam-se:

Detectores de intrusões: *Intrusion Detection System (IDS).* É um dispositivo que gera alerta quando observa tráfegos potencialmente mal-intencionados. Um *IDS* pode ser usado para detectar uma série de tipos de ataques, incluindo mapeamento de rede, escaneamento de portas, *worms* e vírus, escaneamento de pilha TCP, etc. (KUROSE, 2010).

Antivírus: São programas criados para manter os computadores seguros, protegendo-os de programas maliciosos, com o intuito de estragar, *deletar* ou roubar dados do computador. Como exemplos de antivírus destacam-se o *Avira, Panda, McAfee, AVG, TRENDmicro*, etc. A Figura 22 exibe a tela de um programa de antivírus.

Figura 22 – Avira antivírus, protegendo um computador.



Fonte: http://www.techtudo.com.br/

Filtros *anti-spam*: São um conjunto de soluções ou sistemas que analisam as mensagens que chegam a um determinado usuário e, com base em regras ou em verificações de determinados itens, tentam determinar se aquele e-mail é *spam (propagandas não solicitadas)* ou não. Portanto, têm objetivo de tentar bloquear este tipo de mensagem ao mesmo tempo em que permitem que as mensagens legítimas passem. O modo de operação varia de um filtro para outro, assim como a eficiência. A Figura 23 abaixo mostra a caixa de entrada de um e-mail com o ícone do filtro *"spam"* no detalhe, filtro este que às vezes deixa passar alguma mensagem não solicitada ou bloqueia uma mensagem legítima.

Figura 23 – Filtro Anti-*spam* bloqueando mensagens potencialmente prejudiciais.

Fonte: http://www.techtudo.com.br/

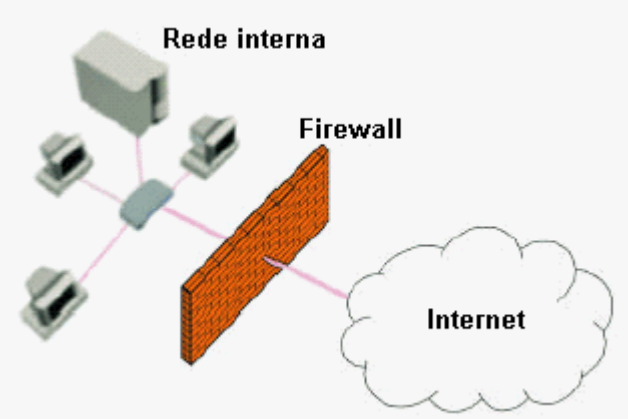
Fuzzers de Segurança: Um *fuzzer* de segurança é uma ferramenta usada por *pentesters* (profissionais de teste de invasão), analistas de segurança e *hackers*, para testar parâmetros de várias aplicações. *Fuzzers* testam *softwares* em busca de erros de programação nos algoritmos. Alguns *fuzzers* avançados incorporam funcionalidades para testar vulnerabilidades do tipo "ataques transversais de pastas", onde o atacante acessa pastas em vários níveis sem privilégios. Fuzzers populares são: *SPIKE Proxy*, *Peach Fuzzer Framework* e *WebScarab*.

Cifragem e Codificação. A cifragem é o processo pelo qual algoritmos são utilizados para “embaralhar” uma “mensagem” tornando a mesma ilegível. A Codificação tem a mesma função, porém, o processo utilizado é um pouco diferente, não existe este embaralhamento, mas sim substituição de “letras, grupos de letras, bits, etc”. Tanto a cifragem como a codificação podem ou não possuir uma chave criptográfica.

Honeypot*:* É uma ferramenta ou sistema criado com objetivo de enganar um atacante e fazê-lo pensar que conseguiu invadir o sistema, quando na realidade, ele está em um ambiente simulado, tendo todos os seus passos vigiados. É uma espécie de armadilha para invasores

Firewall: É qualquer dispositivo destinado a prevenir atacantes externos de acessar sua rede. Este dispositivo pode ser um computador, um roteador, ou um *hardware* dedicado, ou seja, uma combinação de *software e hardware* que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros (Figura 24). *Firewalls* também podem analisar pacotes de vários protocolos e processar os pacotes através de regras que irão permitir ou não a passagem deste pacote.

Figura 24 – Estrutura de atuação de um *Firewall*



Fonte: http://www.projetoderedes.com.br/

Para Nakamura e Geus (2007), o *firewall* é um dos principais, mais conhecidos e antigos componentes de um sistema de segurança. Sua fama de certa forma acaba contribuindo para a criação de uma falsa expectativa quanto à segurança total da organização, além de causar uma mudança ou mesmo uma banalização quanto à sua definição.

3 METODOLOGIA

Esta pesquisa se caracteriza como bibliográfica e documental, descritiva e de caráter *quali*-quantitativo.

Para Fonseca (2002), metodologia é o estudo da organização, dos caminhos a serem percorridos, para se realizar uma pesquisa, estudo, ou para fazer ciência.

A pesquisa, como relata Gil (2007), desenvolve-se por um processo constituído de várias fases, desde a formulação do problema até a apresentação e discussão dos resultados.

Goldenberg (2007), diz que a pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social ou de uma organização.

Em conformidade com Menezes (2009, p. 16), "[...] a pesquisa quantitativa considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisa-las". É também bibliográfica porque como citam Marconi e Lakatos (1999, p. 57), "[...] a pesquisa bibliográfica, ou de fontes secundárias, abrange toda a bibliografia já tornada pública em relação ao tema de estudo [...]", assim, foram consultados os temas voltados para a segurança de informação, como artigos, trabalhos de conclusão de curso, dissertações, periódicos e também os principais bancos de dados de Ciência da Informação.

A pesquisa documental como expõe Kahlmeyer-Mertens, *et al*.(2007), é feita quando se faz necessária a análise de documentos existentes que possam contribuir para a realização da pesquisa.

Com isso, foi realizada a leitura e análise dos principais temas consultados e selecionados os de mais relevância para o presente trabalho, levando em consideração os objetivos proposto a esta pesquisa.

O universo da pesquisa delimitou-se nas 27 bibliotecas universitárias federais brasileiras e para a amostra foram escolhidas seis bibliotecas (Apêndice B).

A coleta dos dados foi feita por meio da ferramenta questionário, o qual é definido Segundo Marconi e Lakatos (1999, p.100), como: "Um instrumento desenvolvido cientificamente, composto de um conjunto de perguntas ordenadas de acordo com um critério predeterminado, respondido sem a presença do entrevistador".

Antes do envio definitivo do questionário, foi realizado um pré-teste em seis (6) bibliotecas escolhidas de forma aleatória entre as 27.

Marconi e Lakatos (2007), dizem que o pré-teste é necessário, pois, evidenciará possíveis falhas existentes como inconsistência ou complexidade das questões; ambiguidade ou linguagem inacessível; perguntas supérfluas, se muito numerosas ou não, dentre outras falhas. Assim, o pré-teste serviu para correção, análise, definição e arranjo das perguntas finais.

Foi elaborado um questionário com 14 questões (Apêndice A) ordenado de acordo com os objetivos específicos da pesquisa e sua aplicação feita através da ferramenta formulário *on line* do *GoogleDrive* e enviado para as 27 bibliotecas universitárias federais brasileiras por meio de e-mail.

As questões foram do tipo fechada e de múltipla escolha, que de acordo com as autoras Marconi e Lakatos (2007), são perguntas fechadas, mas que apresentam uma série de possíveis respostas, abrangendo várias facetas do mesmo assunto.

4 RESULTADOS E ANÁLISE DA PESQUISA

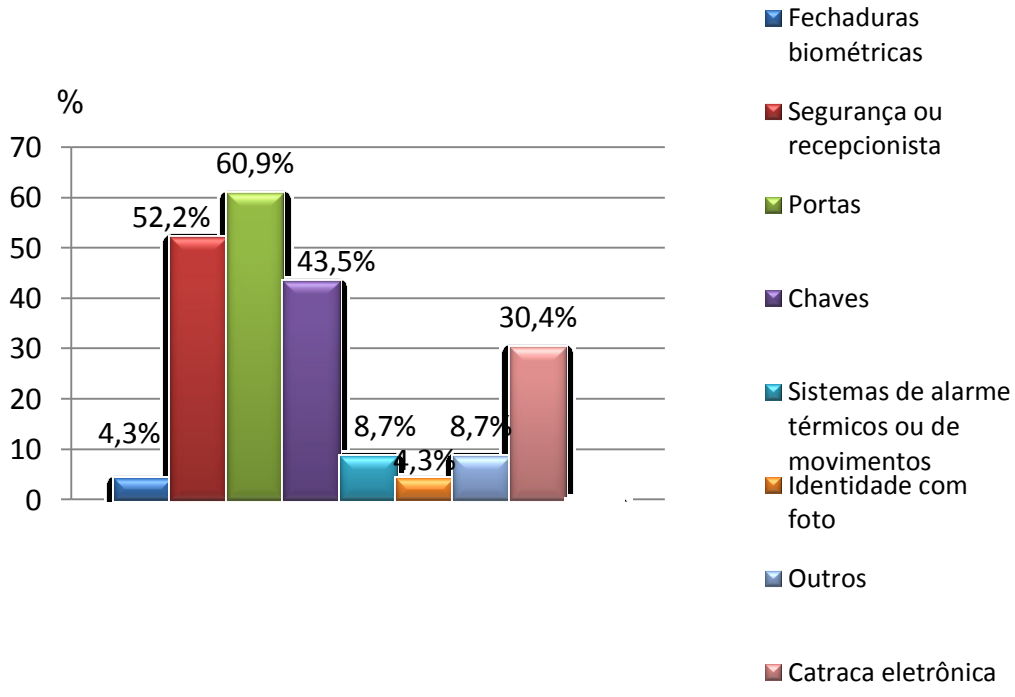
O público alvo do questionário, como já citado, foram as 27 bibliotecas das universidades federais brasileiras (Apêndice B). Destas, somente vinte e uma (21) retornaram o questionário e, como se esperava deste meio de ferramenta de pesquisa, algumas perguntas ficaram sem respostas.

A pergunta 1 do questionário (obrigatória), se referia ao endereço eletrônico da biblioteca, que se fazia necessário para saber a procedência da resposta.

O Gráfico 2 abaixo, representa as respostas da pergunta 2: Quanto à segurança física da BU, qual (ais) o (s) meio (s) de controle de acesso às áreas restritas?

Percebe-se que a maioria, 60,9% dos respondentes possui como controle de acesso apenas portas, seguido de 52,2% dos que possuem segurança ou recepcionistas para o controle. Catraca eletrônica é usada por mais de 30% das bibliotecas, enquanto os demais sistemas não chegam a 10% dos respondentes.

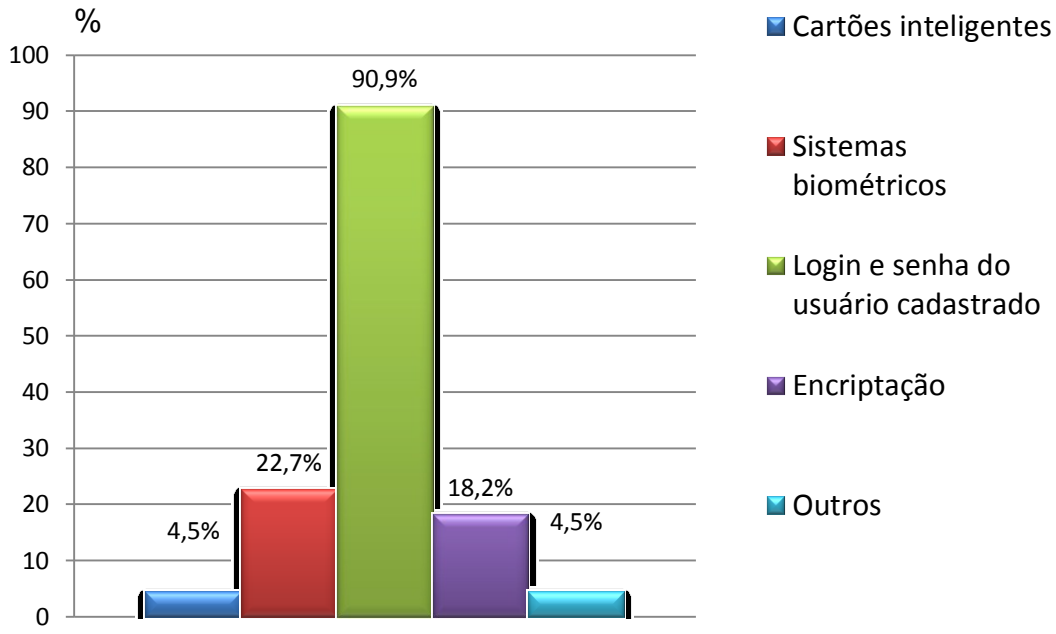
Gráfico 2: Meios de controle de acesso às áreas físicas



Fonte: Gerado a partir do questionário

A pergunta 3 questiona: Quais são as principais técnicas de *softwares* utilizadas no controle lógico de acesso á rede desta unidade? O Gráfico 3 abaixo, demonstra as respostas. Das bibliotecas respondentes, 90% usam apenas *login* e senha de usuários cadastrados. Outras 22,7% usam sistemas biométricos, 18% usam encriptação e, os demais *softwares* utilizados não chegam a 5% de utilização nas bibliotecas.

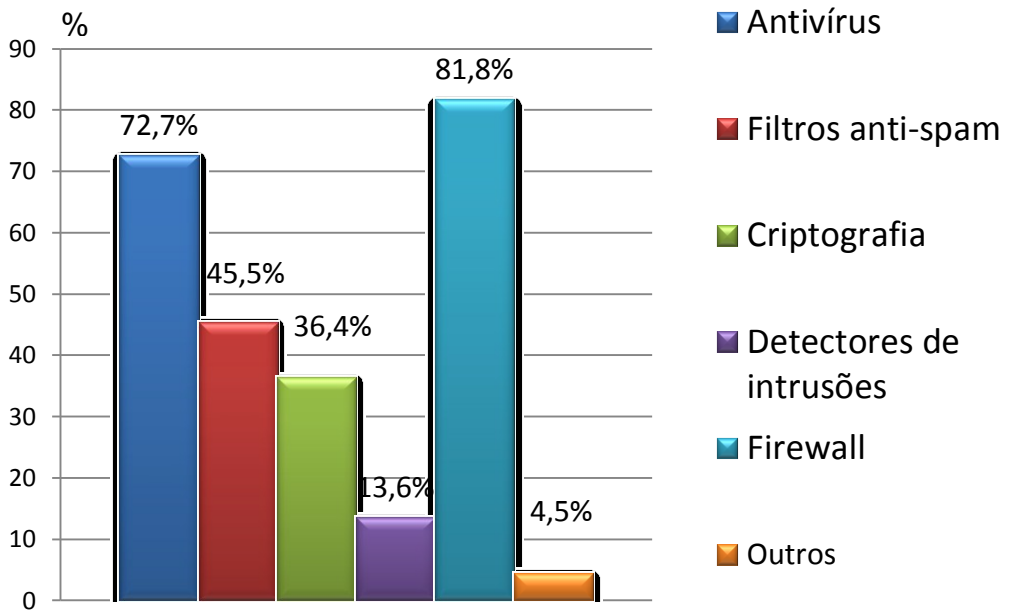
Gráfico 3: *Softwares* utilizados no acesso lógico á rede



Fonte: Gerado a partir do questionário

O Gráfico 4 abaixo, traz a informação das respostas obtidas da pergunta 4 do questionário: Quais as principais ferramentas utilizadas para garantir a segurança ao acesso à rede da BU para seus usuários? Mais de 80% das bibliotecas universitárias federais usam o firewall como a principal ferramenta para garantir a segurança ao acesso à rede de suas instituições, seguido de 72,7% da ferramenta antivírus, e 45,5% dos respondentes usam a ferramenta anti-*spam.* A criptografia também é usada por 36,4% das bibliotecas respondentes. As demais ferramentas não obtiveram 15% de utilização.

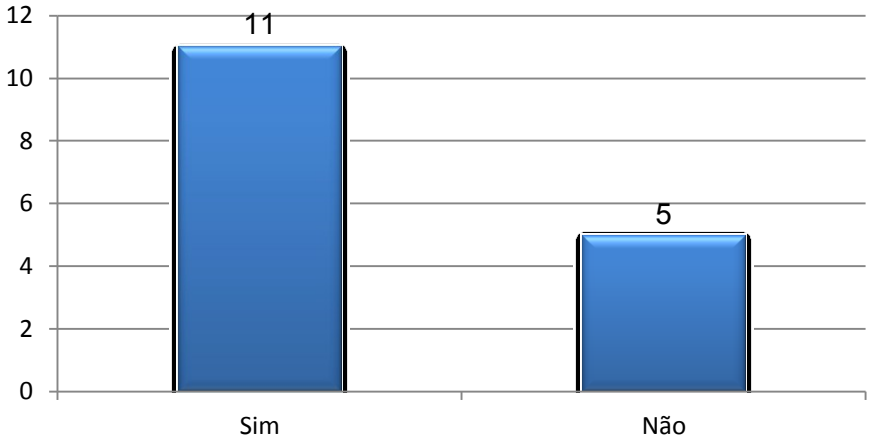
Gráfico 4: Ferramentas utilizadas ao acesso à rede



Fonte: Gerado a partir do questionário

A pergunta 5 é uma questão fechada: Existe um circuito fechado de TV monitorando as principais áreas de acesso aos usuários. As respostas foram: 16 das bibliotecas que responderam a esta questão, 11 disseram que existe, totalizando um percentual de 68,5%. E apenas 5 disseram que não existe, com um percentual de 31,5%, conforme demonstra o Gráfico 5 a seguir.

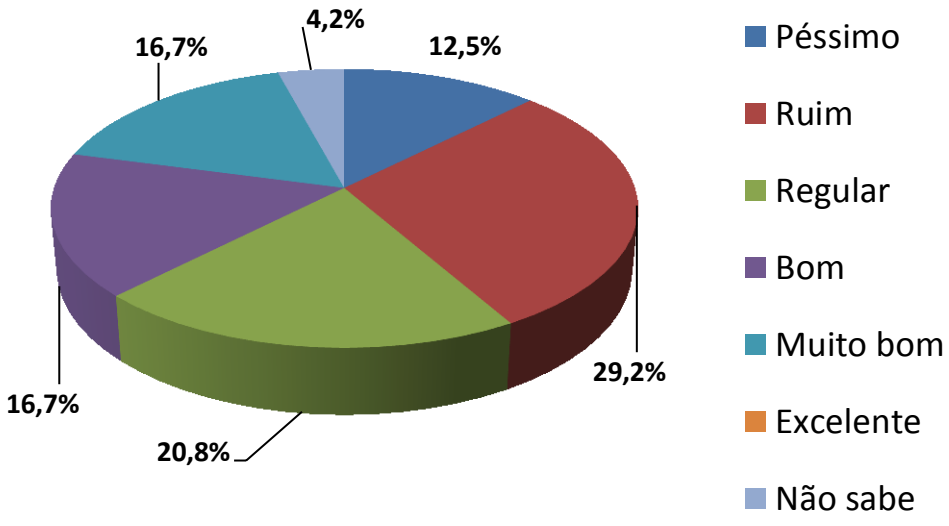
Gráfico 5: Existência de um circuito fechado de tv monitorando áreas de acesso ao usuário



Fonte: Gerado a partir do questionário

A pergunta 6 traz o seguinte enunciado: Na sua opinião, o grau de proteção em segurança da informação na BU hoje é ? O Gráfico 6 abaixo mostra que: 20,8% das instituições possuem um grau de proteção regular em sua segurança da informação. 29,2% tem uma proteção ruim; 16,7% tem uma proteção de boa a muito boa; 12,5% tem uma péssima proteção; 4,2% não sabem e nenhuma tem uma excelente proteção.

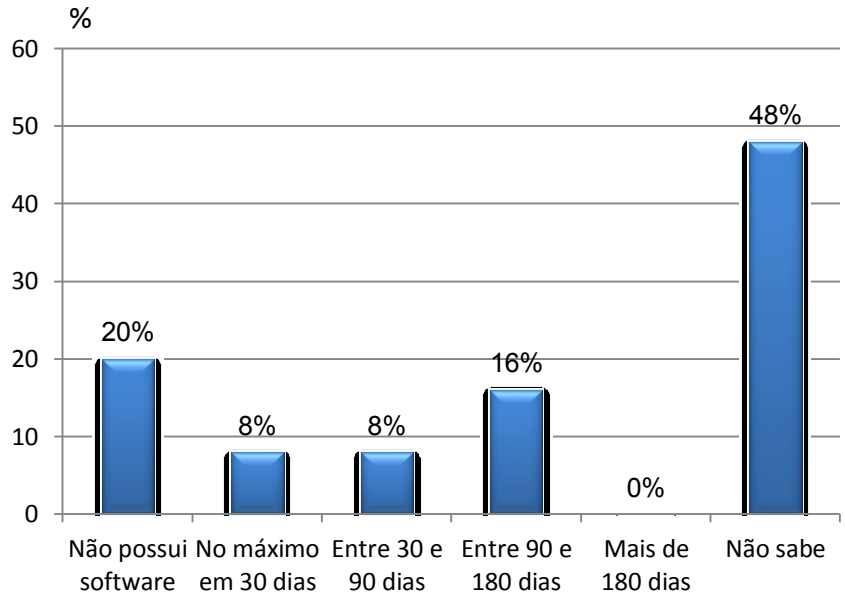
Gráfico 6: Grau de proteção em segurança da informação na biblioteca



Fonte: Gerado a partir do questionário

Qual o tempo médio de atualização dos softwares de segurança, foi a pergunta 7 e se obteve as seguintes respostas conforme mostra o Gráfico 7 abaixo: Em 20% das bibliotecas não possuem software de segurança. Para 8% das bibliotecas, no máximo em 30 dias. Outras 8% entre 30 e 90 dias. Outras que responderam entre 90 e 180 dias soma 16%. Nenhuma respondeu mais de 180 dias, e 48% não sabem o tempo de atualização do software.

Gráfico 7: Tempo de atualização dos softwares

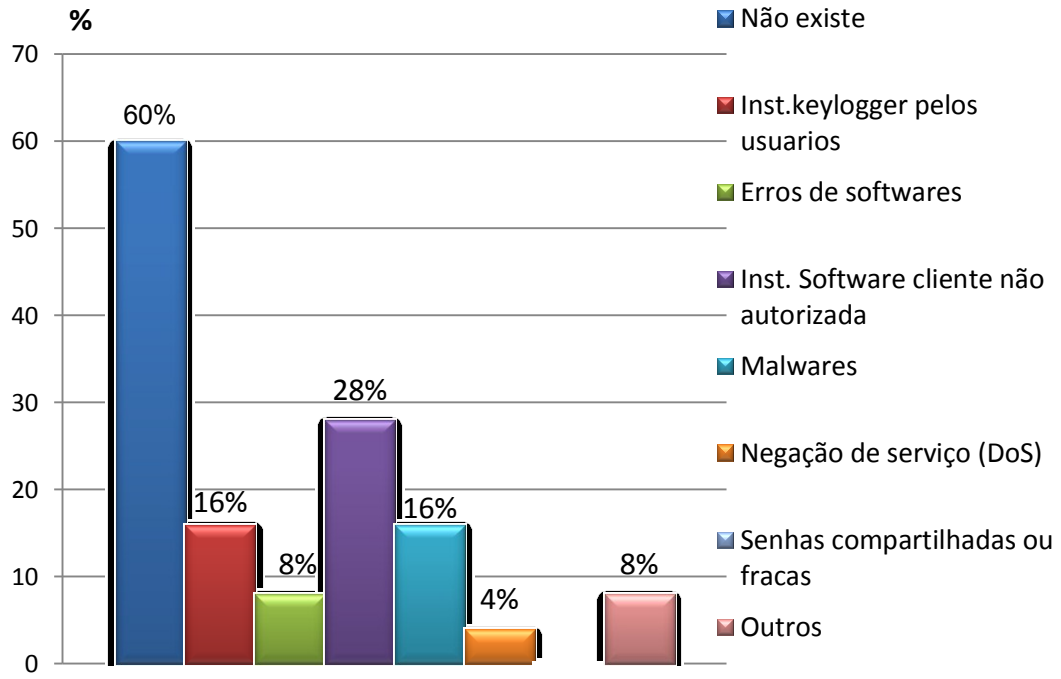


Fonte: Gerado a partir do questionário

Na questão 8, Gráfico 8 a seguir, é perguntado: Existe um sistema de detecção de intrusão para a monitoria das atividades dos usuários tanto internos quanto externos à BU? Se sim, quais os principais incidentes de segurança reportados por este sistema? As respostas mostram que 60% das bibliotecas respondentes não possuem um sistema de detecção de intrusão. 16% disseram que a instalação de *keyloggers* pelos usuários foi o principal incidente reportado. Para 8% dos respondentes foi o erro de softwares. 28% dos respondentes disseram que foi a instalação não autorizada do *software* cliente. Para 16% dos respondentes foram os *malwares.* E 4% das bibliotecas respondentes citaram a negação de

serviço (DoS) como o principal incidente reportado pelo sistema de detecção de intruso.

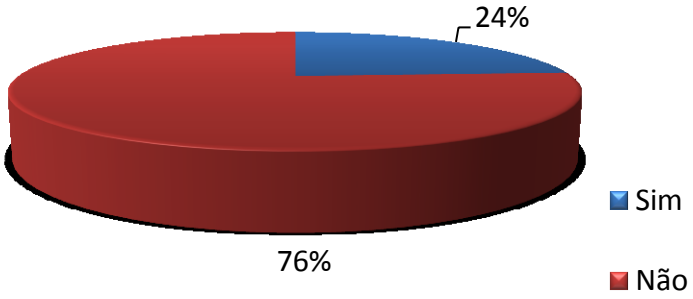
Gráfico 8: Principais incidentes de segurança reportados



Fonte: Gerado a partir do questionário

Para a pergunta 9 – Existe uma política institucional de segurança de informação nesta unidade? O Gráfico 9 a seguir mostra que: em 24% das bibliotecas respondentes existe essa política, mas em 76% das bibliotecas respondentes não existe uma política institucional de segurança da informação.

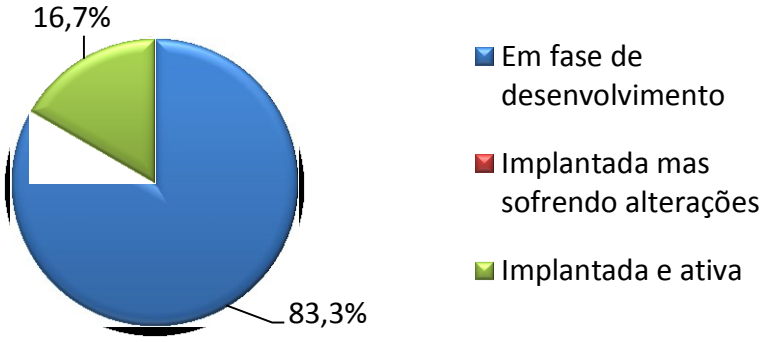
Gráfico 9: Existência de uma política institucional de segurança



Fonte: Gerado a partir do questionário

A pergunta 10 questiona: Se existe uma política de segurança da informação nesta biblioteca ela está: o Gráfico 10 abaixo, deixa claro que em 80,3% das bibliotecas universitárias federais possuem uma política de segurança da informação, embora estejam em fase de desenvolvimento; e 16,7% estão implantadas e ativas.

Gráfico 10 : Existência de uma política de segurança de informação



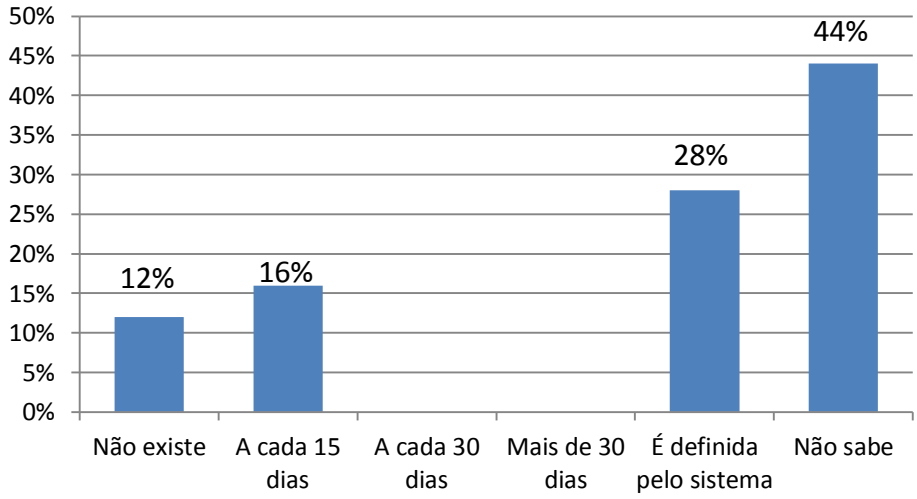
Fonte: Gerado a partir do questionário

A pergunta 11 questiona: Existe algum tipo de planejamento para expansão do sistema de segurança para esta unidade de informação? Se sim, de que tipo? Das 23 bibliotecas respondentes, apenas 11 responderam essa questão, as respostas foram as seguintes:

1-NÃO
1-Há diretrizes elaboradas que visam nortear o uso e manutenção dos computadores no Sistema de Bibliotecas, bem como o acesso à rede Wi-Fi.
1-Não
1-Não!
1-não
1-Sistema de monitoramento por câmeras
1-mudança
1-Não existe
1-Não sei,. Pergunta muito específica
1-Existe um projeto para aquisição de catracas digitais interligadas com o sistema e também sistemas biométricos de identificação para funcionários
1-Monitoramento câmeras e uso de RFID

O Gráfico 11 a seguir mostra qual é a frequência de programação de cópias de segurança de arquivos ou backups das bibliotecas, pergunta 12. Percebe-se que 44% dos respondentes não sabem a frequência. 28% responderam que a frequência é definida pelo sistema. A cada 15 dias 16% responderam. E não existe nenhuma frequência de programação, foi respondido por 12% das bibliotecas.

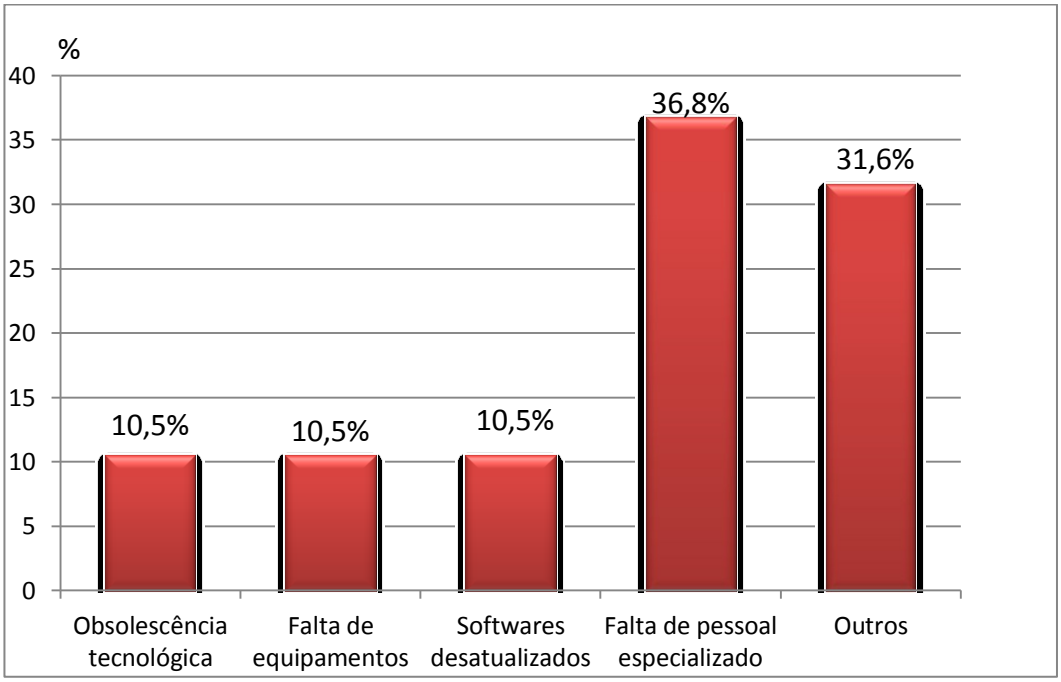
Gráfico 11: Programação de cópias de arquivos



Fonte: Gerado a partir do questionário

As respostas para a pergunta 13: Qual a principal dificuldade em se rastrear ameaças e ataques na rede de sistema de informação da sua unidade? Estão representadas no Gráfico 12 a seguir. Fica claramente evidenciada que a obsolescência tecnológica é a principal dificuldade em se rastrear ataques nas bibliotecas, chegando a 36,8% das bibliotecas respondentes. Outras dificuldades não relacionadas somam 31,6% nas bibliotecas.

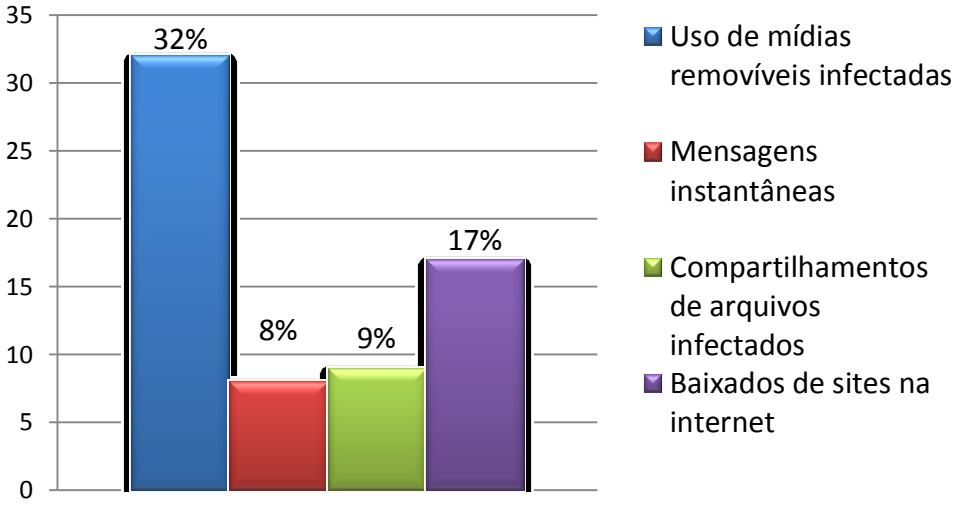
Gráfico 12: Dificuldades em se rastrear ameaças



Fonte: Gerado a partir do questionário

Abaixo, no Gráfico 13, são demonstradas as repostas para a questão 14 do questionário: Qual (ais) a (s) prática (s) mais comum de infecção das pragas virtuais em computadores da biblioteca? Nota-se que a incidência mais comum é pelo uso de mídias removíveis, 32% dos respondentes, e a menor das incidências 8%, é das mensagens instantâneas.

Gráfico 13: Práticas mais comuns de infecção virtual



Fonte: Gerado a partir do questionário

Os resultados mostram, ainda que nem todas as bibliotecas tenham respondido ao questionário, que em sua maioria, há uma grande lacuna a ser preenchida no que se refere a segurança de informação. Os investimentos em proteção por meios eletrônicos, tanto físicos quanto lógicos estão caminhando a passos lentos.

O controle de aceso físico em áreas restritas, por exemplo, na maioria das bibliotecas universitárias ainda acontece por meio de simples portas, (Gráfico 2) ou apenas recepcionistas. Não há um controle mais exigente para o acesso a estas áreas, como leitura biométrica ou *login* e senha. Entretanto, para o controle de acesso lógico à rede das bibliotecas o uso de *login* e senha dos usuários estão presentes em 90% das bibliotecas que responderam ao questionário, conforme mostra o Gráfico 3. Neste campo se nota que o uso de sistemas biométricos e a encriptação já faz parte de uma parcela significativa de bibliotecas que adotam esses controles.

E quanto à segurança aos usuários após o acesso a rede lógica ela é feita principalmente pela ferramenta *firewall* (Gráfico 4) em mais de 80% das bibliotecas. As ferramentas antivírus e *anti-spam* também são as mais usadas para prover a segurança dos usuários na rede, além da criptografia que alcança 36,4% do uso.

Embora a segurança das redes seja uma preocupação presente em todas as bibliotecas, na visão dos bibliotecários que trabalham nestes locais o grau de proteção, de acordo com o Gráfico 6, mostra que quase 30% das bibliotecas respondentes possuem proteção ruim em sua segurança da informação contra 16,7% que têm uma proteção de boa a muito boa.

Este cenário poderia ser mudado se houvessem mais bibliotecas universitárias federais com uma política institucional de segurança de informação, no entanto, o Gráfico 9 deixa claro que em mais de 76% das bibliotecas respondentes não possuem esta política. Muito embora, no Gráfico 10, a política de segurança da informação esteja presente em mais de 80% das bibliotecas questionadas, ela está ativa e implantada em apenas pouco mais de 16%.

Nakamura (2007, p.53), diz: “a segurança da informação é um campo relativamente novo e, muitos ainda não conseguem enxergar a sua importância, imaginando que as soluções são caras e não trazem nenhum retorno financeiro.” Isto bem se aplica a várias instituições, dentre elas as universitárias. O mesmo autor diz ainda que o problema não deve ser se existe ou não segurança e sim em que

nível ela está. Este nível pode definir o quão segura uma instituição está em relação a ataques e invasões virtuais, os grandes vilões da tecnologia na atualidade.

Em relação a esses ataques e invasões, que acontecem diariamente e por diversos meios tecnológicos, as bibliotecas em sua maioria, estão despreparadas para potenciais invasores. O Gráfico 8 por exemplo, mostra que 60% das bibliotecas respondentes não possuem um sistema de detecção de intrusão e com isso, ficam abertas a vários incidentes de segurança em suas redes.

Portanto, se as redes ficam expostas a todo tipo de ataques, se Junta a isso a obsolescência tecnológica que chega a 36,7% das bibliotecas questionadas (Gráfico 12), fica evidente que se torna muito difícil rastrear ameaças e ataques em suas redes de sistema de informação.

Oliveira (2001) lembra que a simples identificação de que o alvo possui algum sistema de defesa, já faz com que invasores menos experientes desistam de sua prática.

5 CONCLUSÕES

A segurança de informação está, assim como a tecnologia, em súbito desenvolvimento. Isto foi possível por meio da globalização da informação e o advento da Internet que alavancou também a preocupação em se manter certos dados seguros, já que o acesso a qualquer tipo de informação hoje em dia é possível por meio de qualquer aparelho eletrônico, como por exemplo, um celular.

Muito se fala em segurança de informação, mas o que se tem feito de fato para assegurar tal proteção é pouco.

No âmbito federal, no caso as bibliotecas das universidades federais brasileiras, a realidade não é diferente. Nos *Campus* universitários, onde o fluxo de acesso à Internet é muito grande, a probabilidade de ataques cibernéticos também é muito real.

Todavia, a criação, ou desenvolvimento de ferramentas e técnicas para uma navegação mais segura na Internet também tem se desenvolvido exponencialmente nas últimas décadas. Com esta preocupação, este trabalho teve como objetivos identificar, determinar e avaliar estas técnicas e ferramentas usadas pelas bibliotecas universitárias federais.

Para a segurança de informação, todo o fator que venha a ser uma ameaça em potencial, é um fator relevante, pois, ela precisa garantir que a informação esteja disponível quando necessária, e que se possa garantir a sua integridade. Este trabalho buscou então, através de questionário enviado para as bibliotecas universitárias federais brasileiras, analisar o nível de segurança em que se encontram os sistemas de segurança de informação dessas instituições assim como o grau de segurança tanto para os usuários que dela necessitam quanto para os bibliotecários que nelas trabalham.

A análise dos resultados obtidos através do questionário traçou um perfil das bibliotecas universidades brasileiras ainda preocupantes. Embora valha destacar que o público alvo inicial era de 27 bibliotecas as quais foram enviados os questionários, apenas 21 retornaram as respostas, ou seja, pouco mais de 77%. Com base neste percentual de respostas foi possível fazer um parâmetro analítico da situação.

A segurança da informação nas bibliotecas universitárias federais está aos poucos se desenvolvendo, como mostrou a pesquisa. Muitas técnicas e ferramentas

de segurança estão chegando e modificando o cotidiano tanto de usuário como o do bibliotecário que precisa estar atuante no processo de transição dessas tecnologias.

A maioria das bibliotecas que responderam ao questionário ainda possui o mínimo de segurança em seus sistemas, estão “abertas” para todo o tipo de ataques e ameaças virtuais. Talvez este seja o reflexo do grande número de obsolescência tecnológica, somada a falta de equipamentos, softwares desatualizados, falta de pessoal especializado e outras tantas dificuldades que as bibliotecas brasileiras sofrem.

Porém, a preocupação em segurança e em se adotar métodos mais seguros, como biometria, encriptação, *backup* de arquivos, sistema de detecção de intrusões e diretrizes que visem o melhoramento de computadores e redes *wi-fi* já é uma realidade em algumas bibliotecas, embora em números ainda tímidos.

Os objetivos da pesquisa foram alcançados, e o resultado mostrou que mesmo com tantas tecnologias e inovações de ponta, muitas vezes tais tecnologias desenvolvidas na própria universidade, a mesma não as usufrui.

Pela dificuldade encontrada na busca por assuntos referente ao tema objeto desta pesquisa, dificuldade esta devido à escassez de artigos publicados, se espera que de alguma maneira, a fundamentação teórica e os resultados aqui apresentados venham a ser úteis para futuras pesquisas tanto de profissionais ou não da Ciência da Informação.

REFERÊNCIAS

ADACHI, Tomi; Orientador: Eduardo Henrique Diniz. **Gestão de Segurança em Internet Banking.** 2004. 121 f. Dissertação (Mestrado) - Curso de Administração, Fundação Getúlio Vargas (fgv), São Paulo, 2004. Disponível em: <http://www.scielo.br/scielo.php?pid=S1807-17752007000300007&script=sci_arttext>. Acesso em: 21 mar. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Norma ISO/ IEC 27001-2006** -Sistemas de Gestão da Segurança da Informação – Requisito, 2006.

_____. NORMA ABNT NBR ISO/IEC 27002- Tecnologia da Informação -Técnicas de Segurança – Código de prática para a gestão da segurança da informação (conteúdo técnico idêntico ao da ABNT NBR ISO/IEC 17799), 2005.

BIANCHETTI, Lucídio. **Da chave de fenda ao laptop:** tecnologia digital e novas qualificações: desafios à educação. 2.ed. ver. e atual. Florianópolis : Ed. da UFSC, 2008.

BITTENCOURT, Thiago. **O que são spywares, vírus, e outros malwares:** como se proteger. 2013. Analista de Sistemas. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.html>. Acesso em: 02 abr. 2015.

BRASIL. INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO (ITI). **DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000:** Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.. Brasília: Diário Oficial da União (d.o.u), 2000. Disponível em: <http://www.iti.gov.br/images/icp-brasil/legislacao/Decretos/DECRETO_3_505_DE_13_06_2000.pdf>. Acesso em: 12 dez. 2014.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações** - São Paulo: Editora SENAC São Paulo, 1999.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERTBR). **Cartilha de segurança para a internet.** Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 24 de setembro de 2014.

CHESWICK, W. ; BELLOVIN, S. M. ; RUBIN. A. D. ; **Firewalls e Segurança na Internet.** 2. ed. RS. Bokman. 2005.

COSTA, Celso; FIGUEIREDO, Luiz Manoel. **Introdução à criptografia.** Rio de Janeiro: Uff, 2010. 100 p.

DIAS, Claudia. **Segurança e auditoria da tecnologia da informação**: Rio de Janeiro: Axcel Books do Brasil, 2000.

ESET-COMPANHIA GLOBAL DE SOLUÇÕES DE SOFTWARE DE SEGURANÇA (São Paulo). **Tipos de Ameaças:** Classificação de Malware. 2012. Disponível em: <http://www.eset.com.br/threat-center/threat-types>. Acesso em: 05 abr. 2015.

FERREIRA, Fernando Nicolau Freitas; ARAúJO, Márcio Tadeu de. **Política de Segurança da Informação:** Guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila. Disponível em: < http://www.ia.ufrrj.br/ppgea/conteudo/conteudo-2012-1/1SF/Sandra/apostilaMetodologia.pdf>. Acesso em: 02 jun. 2015.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2000.172p.

FONTOURA, Paula Renata. **Alan Turing, o pai da computação.** 2012. Portal da Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.invivo.fiocruz.br/cgi/cgilua.exe/sys/start.htm?infoid=1370&sid=7>. Acesso em: 17 dez. 2014.

GARCIA, Gabriel. **5 descobertas de Alan Turing que mudaram o rumo da tecnologia.** 2015. Disponível em: <http://info.abril.com.br/noticias/cultura-nerd/fotonoticias/5-descobertas-de-alan-turing-que-mudaram-o-rumo-da-tecnologia.shtml>. Acesso em: 02 fev. 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

GOLDENBERG, M. **A arte de pesquisar**. Rio de Janeiro: Record, 1997.

IDANKAS, Rodney**. Backup e segurança da informação**. informática, conteúdo especializado em concursos públicos. Maio de 2009. Disponível em: <http://informaticadeconcursos.blogspot.com.br/2009/05/backup-e-seguranca-da-informacao.html>. Acesso em: 10 de outubro de 2014.

INSEGURE.ORG. **As 75 Melhores Ferramentas de Segurança para Sistemas em Rede.** Disponível em:<http://insecure.org/tools/tools-pt.html>. Acesso em: 16 de setembro, 2014.

KAHLMEYER-MERTENS, Roberto S. et al. **Como elaborar projetos de pesquisa:** Linguagem e método. Rio de Janeiro: Fgv, 2007. 140 p.

KUROSE, James F. **Rede de computadores e a internet**: uma abordagem top-down. Tradução de *Opportunity translation*. São Paulo: Addison Wesley, 2010.

LAUREANO, Marcos Aurelio Pchek. **Gestão da Segurança da Informação**. Apostila, 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 12 de jan. de 2015.
MACêDO, Diego. **Mecanismos de controle de acesso.** 2012. Bacharel em Sistemas de Informação pela Estácio de Sá (Alagoas). Disponível em: <http://www.diegomacedo.com.br/mecanismos-de-controle-de-acesso/>. Acesso em: 03 abr. 2015.

MARCONI. M. A.; LAKATOS, E. M. **Técnicas de pesquisa**. São Paulo: Atlas, 1999, p. 100.

MENEZES, Estera Muszkat. **Pesquisa Bibliográfica**– Florianópolis : CIN/CED/UFSC, 2009.

MORIMOTO, Carlos E. **A História da informática (Parte 6: Sistemas embarcados e supercomputadores):** O ENIAC. 2011. Disponível em: <http://www.hardware.com.br/guias/historia-informatica/eniac.html>. Acesso em: 18 nov. 2014.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio de. **Segurança de Redes em ambientes cooperativos.** São Paulo: Novatec, 2007.

NOVAES, Rafael. **Conheça 10 celebridades que tiveram fotos íntimas divulgadas e aprenda a se proteger.** 2015. Blog Psafe. Disponível em: <http://www.psafe.com/blog/conheca-10-celebridades-que-tiveram-fotos-intimas-divulgadas-e-aprenda-a-se-proteger/>. Acesso em: 23 maio 2015.

OLIVEIRA, Wilson Jose de. **Segurança da informação:** técnicas e soluções. Florianópolis: Visual Books, 2001.

OPPERMANN, Álvaro. **Aventuras na História: para viajar no tempo.** 2009. Disponível em: <http://guiadoestudante.abril.com.br/aventuras-historia/linha-tempo-origem-homem-476678.shtml>. Acesso em: 27 jan. 2015.

PÉRICAS, Francisco Adell. **Redes de Computadores:** conceitos e a arquitetura internet. Blumenau: Edifurb, 2003. 158 p.

PINHEIRO, José Maurício S.. **Auditoria e Análise de Segurança da Informação:** Segurança Física e Lógica. 2009. Centro Universitário Geraldo Di Biase (UGB). Disponível em: <http://www.projetoderedes.com.br/aulas/ugb_auditoria_e_analise/ugb_apoio_auditoria_e_analise_de_seguranca_aula_02.pdf>. Acesso em: 03 abr. 2015.

ROSA, Bruno Estêvão. **Segurança da informação.** 2010. Bruno é administrador de sistemas linux, analista de sistemas e CEO do SempiHost - Serviço de hospedagem de sites no Brasil.. Disponível em: <http://www.artigos.com/artigos/artigos-informativos/internet/seguranca-da-informacao-14897/artigo/#.VWu3HtJViko>. Acesso em: 28 maio 2015.

SANTOS, Fabrício. **Controle de Acesso, de quem é a responsabilidade?** 2012. TrustSign Certificadora Digital e Soluções de Segurança da Informação Ltda. Disponível em: <https://www.trustsign.com.br/portal/blog/controle-de-acesso-de-quem-e-a-responsabilidade/>. Acesso em: 04 abr. 2015.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digita**l - Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva - Rio de Janeiro: Campus, 2003.

UCHOA, J. Q. **Segurança Computacional**. UFLA/FAEPE, 2a. Edição. 2005.

WIKIPÉDIA. **Cavalo de Troia.** Disponível em: <https://pt.wikipedia.org/wiki/Cavalo_de_Troia>. Acesso em: 14 jun. 2015.

APÊNDICE A

Questionário TCC

Prezados. Meu nome é Ismael Cabral e sou graduando do curso Bacharelado em Biblioteconomia pela Universidade Federal de Santa Catarina (UFSC), e estou em fase de conclusão do mesmo. Assim, optei por fazer meu trabalho de conclusão de curso (TCC) com o tema relacionado à segurança da informação em bibliotecas universitárias federais brasileiras. Solicito a cooperação para responderem algumas questões que serão relevantes no desenvolvimento do meu trabalho. Suas respostas a este questionário servirão como base para uma melhor definição do trabalho em si. Agradeço de antemão pelas respostas e a atenção dada.

.

*Obrigatório

1 Por favor, identifique sua biblioteca e instituição de ensino. *

2 Quanto à segurança física da BU, qual (ais) o (s) meio (s) de controle de acesso às áreas restritas?

- ☐ Catraca eletrônica
- ☐ Fechadura biométrica
- ☐ Segurança ou recepcionista
- ☐ Cartão de acesso
- ☐ Portas
- ☐ Chaves
- ☐ Sistemas de alarme térmicos ou de movimento
- ☐ Identidades com foto
- ☐ Outro:

3 Quais são as principais técnicas de softwares utilizadas no controle lógico de acesso á rede desta unidade?

- ☐ Encriptação

- ☐ Cartões inteligentes
- ☐ Listas de controle de acesso (Access control lists - ACLs)
- ☐ Software de auditoria de integridade de arquivos
- ☐ Sistemas biométricos
- ☐ Login e senha do usuário cadastrado
- ☐ Outro: _____

4 Quais as principais ferramentas utilizadas para garantir a segurança ao acesso à rede da BU para seus usuários?

- ☐ Anti-vírus
- ☐ Filtros anti-spam
- ☐ Criptografia
- ☐ Fuzzers de segurança
- ☐ Detectores de intrusões
- ☐ Firewall
- ☐ Outro: _____

5 Existe um circuito fechado de TV monitorando as principais áreas de acesso aos usuários?

- ○ Sim
- ○ Não

6 Na sua opinião, o grau de proteção em segurança da informação na BU hoje é ?

- ○ Péssimo
- ○ Ruim
- ○ Regular
- ○ Bom
- ○ Muito bom
- ○ Excelente

- ○ Não sabe

7 Qual o tempo médio de atualização dos softwares de segurança?

- ○ Não possui software
- ○ No máximo em 30 dias
- ○ Entre 30 e 90 dias
- ○ Entre 90 e 180 dias
- ○ Mais de 180 dias
- ○ Não sabe

8 Existe um sistema de detecção de intrusão para a monitoria das atividades dos usuários tanto internos quanto externos à BU? Se sim, quais os principais incidentes de segurança reportados por este sistema?

- ○ Não existe
- ○ Instalação de keyloggers pelos usuários
- ○ Erros de softwares
- ○ Instalação não autorizada do software cliente
- ○ Malwares
- ○ Negação de serviço (DoS)
- ○ Senhas compartilhadas ou fracas
- ○ Outro:

9 – Existe uma política institucional de segurança de informação nesta unidade?

- ○ Sim
- ○ Não

10 -Se existe uma política de segurança da informação nesta biblioteca ela está:

- ○ Em fase de desenvolvimento

- ○ Implantada mas sofrendo alterações
- ○ Implantada e ativa

11 Existe algum tipo de planejamento para expansão do sistema de segurança para esta unidade de informação? Se sim, de que tipo?

12 Qual é a frequência de programação de cópias de segurança de arquivos ou backups?

- ○ Não existe
- ○ A cada 15 dias
- ○ A cada 30 dia
- ○ Mais de 30 dias
- ○ É definida pelo sistema
- ○ Não sabe

13 Qual a principal dificuldade em se rastrear ameaças e ataques na rede de sistema de informação da sua unidade?

- ○ Obsolescência tecnológica
- ○ Falta de equipamentos
- ○ Softwares desatualizados
- ○ Falta de pessoal especializado
- ○ Outro:

14 Qual (ais) a (s) prática (s) mais comum de infecção das pragas virtuais em computadores da biblioteca?

- ○ Mensagens instantâneas
- ○ Uso de mídias removíveis infectadas
- ○ Compartilhamentos de arquivos infectados
- ○ Baixados de sites na internet

APÊNDICE B

Universidades Federais brasileiras e suas respectivas bibliotecas utilizadas nesta pesquisa.

	Unidade federativa	Nome	Sigla	E-mail Biblioteca
1	Distrito Federal	Universidade de Brasília	UnB	direcao@bce.unb.br
2	Goiás	Universidade Federal de Goiás	UFG	asibi1980@gmail.com
3	Mato Grosso	Universidade Federal de Mato Grosso	UFMT	bibliotecacentral@ufmt.br
4	Mato Grosso do Sul	Universidade Federal de Mato Grosso do Sul	UFMS	bibliotecacentral.preg@ufms.br
5	Bahia	Universidade Federal da Bahia	UFBA	bibici@ufba.br
6	Paraíba	Universidade Federal da Paraíba	UFPB	diretoria@biblioteca.ufpb.br
7	Alagoas	Universidade Federal de Alagoas	UFAL	ctic@sibi.ufal.br
8	Pernambuco	Universidade Federal de Pernambuco	UFPE	bcufpe@ufpe.br
9	Sergipe	Universidade Federal de Sergipe	UFS	bicen@ufs.br

	Unidade federativa	Nome	Sigla	E-mail Biblioteca
10	Ceará	Universidade Federal do Ceará	UFC	bu@ufc.br
11	Maranhão	Universidade Federal do Maranhão	UFMA	bibliotecacentral@ufma.br
12	Piauí	Universidade Federal do Piauí	UFPI	bccb@ufpi.edu.br
13	Rio Grande do Norte	Universidade Federal do Rio Grande do Norte	UFRN	bcdir@bczm.ufrn.br
14	Rondônia	Universidade Federal de Rondônia	UNIR	bc-unir@unir.br
15	Roraima	Universidade Federal de Roraima	UFRR	biblioteca.central@ufrr.br
16	Acre	Universidade Federal do Acre	UFAC	cgsi@ufac.br
17	Amapá	Universidade Federal do Amapá	UNIFAP	biblioteca@unifap.br
18	Amazonas	Universidade Federal do Amazonas	UFAM	centralbc@ufam.edu.br
19	Pará	Universidade Federal do Pará	UFPA	bc@ufpa.br
20	Tocantins	Universidade Federal do Tocantins	UFT	coordbiblio@uft.edu.br

	Unidade federativa	Nome	Sigla	E-mail Biblioteca
21	Minas Gerais	Universidade Federal de Minas Gerais	UFMG	bu-bcentral@ufmg.br
22	São Paulo	Universidade Federal de São Paulo	UNIFESP	biblioteca.csp@unifesp.br
23	Espírito Santo	Universidade Federal do Espírito Santo	UFES	biblioteca@bc.ufes.br
24	Rio de Janeiro	Universidade Federal do Rio de Janeiro	UFRJ	sibi@sibi.ufrj.br
25	Santa Catarina	Universidade Federal de Santa Catarina	UFSC	diretor.bu@contato.ufsc.br
26	Paraná	Universidade Federal do Paraná	UFPR	saubc@ufpr.br
27	Rio Grande do Sul	Universidade Federal do Rio Grande do Sul	UFRGS	bcentral@bc.ufrgs.br